ACTA ARITHMETICA
109.3 (2003)

# Unique range sets and uniqueness polynomials in positive characteristic

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 $f \equiv g$. The following properties are immediate consequences of the definitions:

(P1) *If $\mathcal{F} \subset \mathcal{F}' \subset \mathcal{M}^*(\mathbf{k})$ then a finite set $S$ in $\mathbf{k}$ being a unique range set for $\mathcal{F}'$ implies that it is also a unique range set for $\mathcal{F}$.*

(P2) *If $\mathcal{F} \subset \mathcal{F}' \subset \mathcal{M}^*(\mathbf{k})$ then a polynomial $P$ being a* (*strong*) *uniqueness polynomial for $\mathcal{F}'$ implies that it is also a* (*strong*) *uniqueness polynomial for $\mathcal{F}$.*

In studying unique range sets for $\mathcal{A}^*(\mathbf{k})$ = non-constant entire functions defined over $\mathbf{k}$, one is naturally led to the following polynomial:

$$P_S(X) = (X - s_1)\ldots(X - s_n) \tag{1.1}$$

where $S = \{s_1, \ldots, s_n\}$ is a finite subset of $\mathbf{k}$. Suppose that $f, g \in \mathcal{A}^*(\mathbf{k})$ are

2000 *Mathematics Subject Classification*: Primary 12E05; Secondary 11S80, 30D35.

two entire functions sharing $S$ counting multiplicity. Then $P_S(f)$ and $P_S(g)$ are non-archimedean entire functions with exactly the same zeros counting multiplicity. This implies that $P_S(f)/P_S(g)$ is entire and non-vanishing, hence must be a constant. This shows that:

(P3) *With respect to the family of non-constant entire functions* $\mathcal{A}^*(\mathbf{k})$, *a finite set* $S$ *is a unique range set counting multiplicity if and only if its associated polynomial*, *defined by* (1.1), *is a strong uniqueness polynomial.*

Let $S$ be a subset of $\mathbf{k}$ of finite cardinality $n$. If $p = 0$, or if $p > 0$ and does not divide $n$, then $S$ is a unique range set counting multiplicity for $\mathcal{A}^*(\mathbf{k})$ if and only if $S$ is *affine rigid*, i.e. the only affine transformation preserving the set $S$ is the identity. This result was first proved by Boutabaa, Escassut and Haddad [4] for the case of polynomials, extended by Cherry and Yang [7] to entire functions, in characteristic zero; and, in positive characteristic, by Voloch (cf. the appendix in [8]). If $p > 0$ divides $n$, this geometric characterization of finite unique range sets counting multiplicity for $\mathcal{A}^*(\mathbf{k})$ is no longer valid; counter-examples were provided in [2] and [7]. Let $S = \{s_1, \ldots, s_n\}$ with $n$ divisible by $p$. In this paper we give a complete characterization for $S$ to be a unique range set counting multiplicity for $\mathcal{A}^*(\mathbf{k})$ if the associated polynomial $P_S$ satisfies one of the following two conditions:

(1) $P_S'(X) = \lambda(X-\alpha)^{m-1} \not\equiv 0$ and the multiplicity of $P_S(X)$ at $X - \alpha$ is strictly less than $m$ which is prime to $p$;

(2) $P_S(X)$ is of the form $(X-\alpha)^n + a(X-\alpha)^m + b$ where $m$ is prime to $p$.

There are several reasons to study polynomials of these two types. First of all, we will see later that if $P_S'(X) = \lambda(X-\alpha)^{m-1}$, $m$ relatively prime to $n$, then the set $S$ is affine rigid. Secondly, in [8] the second named author has shown that when $p \mid n$, if (a) $P_S(X)$ is injective on the zeros of $P_S'(X) = \lambda(X-\alpha_1)^{m_1} \ldots (X-\alpha_l)^{m_l}$, (b) the degree of $P_S'(X)$ is $n-2$, and (c) the multiplicity of $X - \alpha_i$ in $P(X) - P(\alpha_i)$ is $m_i + 1$, for $1 \le i \le l$, then $P_S$ is a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$ if and only if $l \ge 2$ and $S$ is affine rigid. Therefore, if one looks for a set which is affinely rigid, but not a unique range set, it is natural to start with those $S$ with $l = 1$ (note that Example 2.2 of [2] satisfies the condition $l = 1$). Thirdly, when $l = 1$, the injective condition on the zero of $P_S'(X)$ always holds. Hence this is a good example to see the impact of the conditions (b) and (c).

The main results in this paper are as follows. We always assume that $\mathbf{k}$ is an algebraically closed field of characteristic $p > 0$, complete with respect to a non-archimedean absolute value.

THEOREM 1. *Let* $S$ *be a finite set in* $\mathbf{k}$ *with associated polynomial* $P_S$. *Assume that* $\#S = n$ *is divisible by* $p$ *and* $P_S'(X) = \gamma(X-\alpha)^{m-1}$, $\alpha \in \mathbf{k}$, *where $\gamma \neq 0$, $m \geq 2$ is relatively prime to $n$, and $P_S(\alpha) \neq 0$. Then $S$ is affine rigid.*

THEOREM 2. *Let $S$ be a finite subset of $\mathbf{k}$ with associated polynomial $P_S$. Assume that* (i) *$\#S = n$ is divisible by $p$,* (ii) *$P_S'(X) = \gamma(X-\alpha)^{m-1}$ where $\gamma \neq 0$ and $m$ is relatively prime to $n$,* (iii) *$P_S(\alpha) \neq 0$, and* (iv) *the multiplicity of $X-\alpha$ in $P_S(X) - P_S(\alpha)$ is strictly less than $m$. Then $P_S$ is a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$; in particular, $S$ is a unique range set for $\mathcal{A}^*(\mathbf{k})$.*

The polynomial $P_S$ satisfies the conditions of Theorem 2 if and only if $\#S = n$ is divisible by $p$ and $P_S$ is of the form

$$P_S(X) = \sum_{0\leq i\leq n} a_i(X-\alpha)^{n_i} + a(X-\alpha)^m + b, \qquad ab \neq 0,\ a_i \neq 0,\ p \mid n_i, \tag{1.2}$$

where $m, n$ are relatively prime and there exists $n_i$ such that $n_i < m$. For example, if $p = 2$ then $X^4 + X^2 + X^3 + 1$ satisfies all the conditions of Theorem 2 but $X^4 + X^2 + X + 1$ does not. Some special examples satisfying the hypothesis of Theorem 2 were treated by various authors using the classical genus formula. We are able to arrive at this more general form by using a new technique which we call the Wronskian construction (see Section 3 for details).

THEOREM 3. *Let $S$ be a finite subset of $\mathbf{k}$ with $n$ elements and $n$ divisible by $p$. Suppose that its associated polynomial is of the form*

$$P_S(X) = (X-\alpha)^n + a(X-\alpha)^m + b$$

*where $m$ is relatively prime to $n$, $a \neq 0$, and $b \neq 0$. Then:*

(1) *$S$ is a unique range set for $\mathcal{A}^*(\mathbf{k})$ if and only if either*

  (a) *$n = p^r s$, $p \nmid s$, $s \geq 2$ and $m \geq 1$, or*
  (b) *$n = p^r$ and $3 \leq m \leq n-2$.*

(2) *$P_S$ is a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$ if and only if $P_S$ is a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$ if and only if either*

  (a) *$n = p^r$ and $3 \leq m \leq n-2$ except $m = 3$ and $n = 5$, or*
  (b) *$n = p^r s$, $p \nmid s$, $s \geq 2$ and $1 \leq m \leq n-2$ except $m = 1$ and $s = 2$.*

Note that the polynomial in Theorem 3 satisfies all the hypothesis of Theorem 2 but (iv).

**2. Proof of Theorem 1 and some basic reductions.** We have seen that $S$ is a unique range set counting multiplicity for $\mathcal{A}^*(\mathbf{k})$ if and only if its associated polynomial $P_S$ is a strong uniqueness polynomial. Let $P(X)$ be a monic polynomial of degree $n$ in $\mathbf{k}[X]$; we introduce the following functions:

$$(2.1)\qquad \begin{cases} F(X,Y) = (P(X) - P(Y))/(X - Y), \\ F_c(X,Y) = P(X) - cP(Y), \quad c \neq 0, 1 \text{ is a constant.} \end{cases}$$

Denote by $F(X,Y,Z)$ and $F_c(X,Y,Z)$ respectively, the homogenizations of $F(X,Y)$ and $F_c(X,Y)$.

The following fact was observed by Cherry and Yang in [7]. For the convenience of the reader, we include their proof.

PROPOSITION 1. (1) *A polynomial* $P \in \mathbf{k}[X]$ *is a* (*strong*) *uniqueness polynomial for* $\mathcal{M}^*(\mathbf{k})$ *if and only if it is a* (*strong*) *uniqueness polynomial for the family of non-constant rational functions in* $\mathbf{k}(t)$.

(2) *A polynomial* $P \in \mathbf{k}[X]$ *is a* (*strong*) *uniqueness polynomial for* $\mathcal{A}^*(\mathbf{k})$ *if and only if it is a* (*strong*) *uniqueness polynomial for the family of non-constant polynomials* $\mathbf{k}[t]$.

*Proof.* Suppose that $P$ is not a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$. Then $F(f,g) = 0$ for some $f, g \in \mathcal{M}^*(\mathbf{k})$. Therefore there is an irreducible factor $F_0(X,Y)$ of $F(X,Y)$ with $F_0(f,g) = 0$. Then by Berkovich's non-archimedean Picard Theorem (cf. [1] and also [6] for a more elementary proof), $F_0(X,Y) = 0$ is a rational curve, and it can be rationally parametrized since $\mathbf{k}$ is algebraically closed. In other words, there exist rational functions $r(t)$, $s(t)$, and $R(X,Y)$ such that $t = R(X,Y)$, and $F_0(r(t), s(t)) = 0$. This shows that $P(X)$ is not a uniqueness polynomial for the family of non-constant polynomials $\mathbf{k}[t]$. The converse is clear.

For (2), we assume that $f, g \in \mathcal{A}^*(\mathbf{k})$. From the previous deduction, we let $h = R(f,g)$, so that $f = r(h)$, and $g = s(h)$. Since $f$ and $g$ are entire, the non-archimedean meromorphic function $h$ must omit the poles of $r(t)$ and the poles of $s(t)$. However, a non-constant non-archimedean meromorphic function can omit at most one point in $\mathbf{k} \cup \{\infty\}$. Thus the $r(t)$ has only one pole which is also the unique pole of $s(t)$. Therefore, after making a projective linear change in coordinates, we can assume that this pole is $\infty$. Therefore, $r(t)$ and $s(t)$ are polynomials. Moreover, $h$ is entire since it omits the pole of $r(t)$. This shows that if $P$ is not a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$, then it is not a uniqueness polynomial for the family of non-constant polynomials $\mathbf{k}[t]$. The converse is clear.

The proof for strong uniqueness is similar. ∎

To prove that a polynomial is a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$, it suffices to show that the curves $F(X,Y,Z) = 0$ and $F_c(X,Y,Z) = 0$ have no irreducible component of genus 0. It was also observed by Cherry and Yang in [7] that a (strong) uniqueness polynomial for the family of polynomials over $\mathbf{k}$ is also a (strong) uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$.

We refer to [8] for a proof of the following result:

PROPOSITION 2. *Let $S$ be a finite set in $\mathbf{k}$ and assume that $P'_S(X)$ is not identically zero. Then $S$ is affine rigid if and only if neither $F(X,Y)$ nor $F_c(X,Y)$, $c \neq 0,1$, has a linear factor.*

PROPOSITION 3. *Let $\mathcal{F}$ be a subset of $\mathcal{M}^*(\mathbf{k})$ and $P(X)$ a polynomial. Then*

(1) *if $S$ is a finite set of $\mathbf{k}$, then the zero set of $P_S(X)$ is affine rigid if and only if the zero set of $P_S(aX+b)$, where $a,b \in \mathbf{k}$ and $a \neq 0$, is affine rigid*;

(2) *$P(X)$ is a uniqueness polynomial for $\mathcal{F}$ if and only if $aP(X)+b$, where $a,b \in \mathbf{k}$ and $a \neq 0$, is a uniqueness polynomial for $\mathcal{F}$*;

(3) *if the family $\mathcal{F}$ satisfies the condition that $f \in \mathcal{F}$ implies that $af+b \in \mathcal{F}$ for any $a,b \in \mathbf{k}$, $a \neq 0$, then $P(X)$ is a strong uniqueness polynomial for $\mathcal{F}$ if and only if $Q(X) = P(aX+b)$ is a strong uniqueness polynomial for $\mathcal{F}$ where $a,b \in \mathbf{k}$ and $a \neq 0$.*

*Proof.* Assertion (2) is clear. For (1), let $S = \{s_1, \ldots, s_n\}$. Then

$$\begin{aligned} P_S(aX+b) &= (aX+b-s_1)\ldots(aX+b-s_n) \\ &= a^n\left(X + \frac{b-s_1}{a}\right)\ldots\left(X + \frac{b-s_n}{a}\right). \end{aligned}$$

Assertion (1) follows from this and the fact that $S$ is affine rigid if and only if $a^{-1}(S-b)$ is affine rigid. For (3) it suffices to show that if $P(X)$ is not a strong uniqueness polynomial then neither is $Q(X) = P(aX+b)$. Suppose that $P(f) = cP(g)$, $c \neq 0 \in \mathbf{k}$, for a pair of distinct functions in $\mathcal{F}$. Let $f_0 = a^{-1}(f-b)$ and $g_0 = a^{-1}(g-b)$. Then $f_0, g_0 \in \mathcal{F}$, $f_0 \neq g_0$, and $Q(f_0) = Q(g_0)$. ∎

PROPOSITION 4. *Let $P(X)$ be a polynomial of degree $n$ divisible by $p$ and $P(0) \neq 0$. Suppose that $P'(X) = \gamma X^{m-1}$ for some $m \geq 2$ relatively prime to $n$ where $\gamma$ is a non-zero constant. Then the polynomials $F(X,Y)$ and $F_c(X,Y)$, $c \neq 0,1$, have no linear factors. Equivalently, the zero set of $P(X)$ is affine rigid.*

*Proof.* We first claim that if $F(X,Y)$ or $F_c(X,Y)$ has a linear factor $X-aY-b$ with $a \neq 0$, then $P(aY+b) = \alpha P(Y)$ where $\alpha = 1$ if $X-aY-b$ is a linear factor of $F(X,Y)$; and $\alpha = c$ if $X-aY-b$ is a linear factor of $F_c(X,Y)$. Indeed, $F(X,Y) = (X-aY-b)Q(X,Y)$ for a polynomial $Q(X,Y)$ if and only if $P(X)-P(Y) = (X-Y)(X-aY-b)Q(X,Y)$. For $X = aY+b$ the right hand side is zero and we have $P(aY+b) = P(Y)$ (so $\alpha = 1$). Similarly $F_c(X,Y) = (X-aY-b)R(X,Y)$ for a polynomial $R(X,Y)$ if and only if $P(X)-cP(Y) = (X-aY-b)R(X,Y)$. For $X = aY+b$ the right hand side is zero and we have $P(aY+b) = cP(Y)$ (so $\alpha = c$, recall that $c \neq 0,1$).

On the other hand, differentiation of $P(aY+b)=\alpha P(Y)$ shows that $a(aY+b)^{m-1}=\alpha Y^{m-1}$, hence $b=0$ (by the assumption that $m\geq 2$) and $a^m=\alpha$, i.e., $P(aY)=\alpha P(Y)$. Comparing the leading coefficients and the constant terms of $P(aY)$ and $\alpha P(Y)$, we see that $a^n=\alpha$, and $\alpha=1$ since $P(0)\neq 0$. Thus $a^n=a^m=\alpha=1$. But in the case of $F_c(X,Y)$ we have $\alpha=c\neq 1$, thus $F_c(X,Y)$ with $c\neq 1$ cannot have a linear factor $X-aY-b$. Since $m$ and $n$ are relatively prime, the condition that $a^n=a^m=\alpha=1$ implies that $a=1$. Thus

$$\frac{P(X)-P(Y)}{X-Y}=F(X,Y)=(X-aY-b)Q(X,Y)=(X-Y)Q(X,Y)$$

which implies that $P'(X)=F(X,X)\equiv 0$, contradicting our assumption on $P'(X)$. Thus $F(X,Y)$ cannot have a linear factor either. ∎

*Proof of Theorem 1.* Let $Q(X)=P_S(X+\alpha)$. Then $Q(0)\neq 0$ and $Q'(X)=P_S'(X+\alpha)=\gamma X^{m-1}$. Thus the polynomial $Q$ satisfies the hypothesis of Proposition 4, hence the zero set of $Q(X)$ is affine rigid. By part (1) of Proposition 3 the zero set of $P_S(X)$ is also affine rigid. ∎

**3. 1-forms of Wronskian type and the proof of Theorem 2.** Consider the problem of computing the genus of a curve in $\mathbf{P}^2(\mathbf{k})$. The case of a smooth curve is easily computed via the genus formula $g=(q-1)(q-2)/2$ where $q$ is the degree of the smooth curve. Note that $(q-1)(q-2)/2$ is the number of distinct monomials of degree $q$ in $z_0,z_1$ and $z_2$. There is also a genus formula for irreducible singular curves in terms of the Milnor number of an isolated singularity and the number of local branches at the singular point. It is usually quite a chore to compute these invariants, and worst of all is the condition that the curve be irreducible. For this reason we develop a procedure of computing the genus without a priori knowledge of irreducibility. The main idea is based on modifying the rational 1-forms

$$\frac{\begin{vmatrix} z_i & z_j \\ dz_i & dz_j \end{vmatrix}}{z_j^2}=\frac{z_i}{z_j}\begin{vmatrix} 1 & 1 \\ \frac{dz_i}{z_i} & \frac{dz_j}{z_j} \end{vmatrix}=d\left(\frac{z_i}{z_j}\right),\qquad i\neq j$$

(where $[z_0,z_1,z_2]$ are the homogeneous coordinates of $\mathbf{P}^2(\mathbf{k})$), or more generally rational 1-forms of the type

$$\beta d\left(\frac{z_j}{z_k}\right)-\alpha d\left(\frac{z_i}{z_k}\right)=\begin{vmatrix} 1 & 1 \\ \alpha d(\frac{z_i}{z_k}) & \beta d(\frac{z_j}{z_k}) \end{vmatrix},\qquad 0\leq i,j,k\leq 2,\ \alpha,\beta\in\mathbf{k}.$$

Any rational 1-form on $\mathbf{P}^2(\mathbf{k})$ is a linear combination of these forms (over the rational function field). We introduce formally the notion of 1-forms of Wronskian type:

Definition 1. Let $C$ be a curve in $\mathbf{P}^2(\mathbf{k})$. A differential 1-form $\omega$ on $C$ is said to be a *1-form of Wronskian type* if $\omega = (fdg - gdf)h$ for some $f$, $g$, and $h$ in the function field of $C$.

We look for polynomials $P$ such that the curves defined by $F(X,Y,Z) = 0$ (resp. $F_c(X,Y,Z) = 0, c \neq 0,1$) have no linear component. Then we construct, on each of these curves, a 1-form $\omega$ of Wronskian type whose restriction to the curve is regular. If $C$ has a rational irreducible component $L$ then the pull-back of $\omega$ to $L$ must be identically zero, as there are no non-trivial regular 1-forms on a rational curve. The Wronskian condition implies that if $f$ and $g$ are rational functions such that the image of the map $\phi$ defined by $(f,g,1)$ is contained in $C = F(X,Y,1)$ then either $f$ and $g$ are $p$th powers or the image of $\phi$ is contained in a line (see the proof of Lemmas 1 and 2 below).

Let $Q(X,Y,Z)$ be a non-trivial homogeneous polynomial in $X$, $Y$, $Z$ and $C = [Q = 0]$ be the curve defined by $Q$. By Euler's Theorem the condition $Q = 0$ is equivalent to

$$X\frac{\partial Q}{\partial X}(X,Y,Z) + Y\frac{\partial Q}{\partial Y}(X,Y,Z) + Z\frac{\partial Q}{\partial Z}(X,Y,Z) = 0. \tag{3.1}$$

The (Zariski) tangent space of $C$ is defined by the equations $Q = 0$ and

$$\frac{\partial Q}{\partial X}(X,Y,Z)dX + \frac{\partial Q}{\partial Y}(X,Y,Z)dY + \frac{\partial Q}{\partial Z}(X,Y,Z)dZ = 0. \tag{3.2}$$

If $\frac{\partial Q}{\partial X}(X,Y,Z) \not\equiv 0$, $\frac{\partial Q}{\partial Y}(X,Y,Z) \not\equiv 0$, $\frac{\partial Q}{\partial Z}(X,Y,Z) \not\equiv 0$, then, by Cramer's rule,

$$\frac{\begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}}{\frac{\partial Q}{\partial Z}(X,Y,Z)} \equiv \frac{\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}}{\frac{\partial Q}{\partial X}(X,Y,Z)} \equiv \frac{\begin{vmatrix} Z & X \\ dZ & dX \end{vmatrix}}{\frac{\partial Q}{\partial Y}(X,Y,Z)} \tag{3.3}$$

defines a rational 1-form of Wronskian type on $\pi^{-1}(C)$ where $\pi : \mathbf{k}^3 \setminus \{0\} \to \mathbf{P}^2(\mathbf{k})$ is the projection map. More precisely, each of the rational 1-forms

$$\frac{\begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}}{\frac{\partial Q}{\partial Z}(X,Y,Z)}, \quad \frac{\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}}{\frac{\partial Q}{\partial X}(X,Y,Z)}, \quad \frac{\begin{vmatrix} Z & X \\ dZ & dX \end{vmatrix}}{\frac{\partial Q}{\partial Y}(X,Y,Z)}$$

is well defined on $\mathbf{k}^3 \setminus \{0\}$ and the identity (3.3) says that the pull-backs of these 1-forms to $\pi^{-1}(C)$ are identical. To realize these forms defined on $\mathbf{k}^3 \setminus \{0\}$ as forms on $\mathbf{P}^2(\mathbf{k})$ we replace the homogeneous coordinates by inhomogeneous ones. For example,

$$\frac{\begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}}{\frac{\partial Q}{\partial Z}(X,Y,Z)} = \frac{XdY - YdX}{\frac{\partial Q}{\partial Z}(X,Y,Z)} = -\frac{X^2}{\frac{\partial Q}{\partial Z}(X,Y,Z)}\, d\left(\frac{Y}{X}\right)$$

where $d(Y/X)$ is a well defined rational 1-form on $\mathbf{P}^2(\mathbf{k})$ because $Y/X$ is a well defined rational function on $\mathbf{P}^2(\mathbf{k})$. Suppose that $\deg Q = q \geq 3$. Then, for any homogeneous polynomial $R$ of degree $q-3$, $X^2R/(\partial Q/\partial Z)$ is a well defined rational function on $\mathbf{P}^2(\mathbf{k})$, hence

$$R(X,Y,Z)\frac{\begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}}{\frac{\partial Q}{\partial Z}(X,Y,Z)} = -\frac{X^2R(X,Y,Z)}{\frac{\partial Q}{\partial Z}(X,Y,Z)}\,d\left(\frac{Y}{X}\right)$$

is a well defined rational 1-form of Wronskian type on $\mathbf{P}^2(\mathbf{k})$. If $\deg Q \leq 3$ then for any homogeneous polynomial $R$ of degree $3-q$,

$$\frac{1}{R(X,Y,Z)}\frac{\begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}}{\frac{\partial Q}{\partial Z}(X,Y,Z)} = -\frac{X^2}{R(X,Y,Z)\frac{\partial Q}{\partial Z}(X,Y,Z)}\,d\left(\frac{Y}{X}\right)$$

is a well defined rational 1-form of Wronskian type on $\mathbf{P}^2(\mathbf{k})$. Suppose that $f_i$, $0 \leq i \leq 2$ (at least one of them not identically zero), are non-archimedean entire functions such that $Q(f_0, f_1, f_2) \equiv 0$, i.e., the image of the map $f = [f_0, f_1, f_2] : \mathbf{k} \to \mathbf{P}^2(\mathbf{k})$ is contained in $C$. Then we have

$$\begin{aligned} f_0\,\frac{\partial Q}{\partial X}(f_0,f_1,f_2) + f_1\,\frac{\partial Q}{\partial Y}(f_0,f_1,f_2) + f_2\,\frac{\partial Q}{\partial Z}(f_0,f_1,f_2) &= 0,\\ f_0'\,\frac{\partial Q}{\partial X}(f_0,f_1,f_2) + f_1'\,\frac{\partial Q}{\partial Y}(f_0,f_1,f_2) + f_2'\,\frac{\partial Q}{\partial Z}(f_0,f_1,f_2) &= 0. \end{aligned}$$

If all three partial derivatives $\frac{\partial Q}{\partial X}(f_0,f_1,f_2)$, $\frac{\partial Q}{\partial Y}(f_0,f_1,f_2)$, $\frac{\partial Q}{\partial Z}(f_0,f_1,f_2)$ are not identically zero, then by Cramer's rule, we have

$$\frac{W(f_0,f_1)}{\frac{\partial Q}{\partial Z}(f_0,f_1,f_2)} \equiv \frac{W(f_1,f_2)}{\frac{\partial Q}{\partial X}(f_0,f_1,f_2)} \equiv \frac{W(f_2,f_0)}{\frac{\partial Q}{\partial Y}(f_0,f_1,f_2)} \tag{3.4}$$

where

$$W(f_i,f_j) := \begin{vmatrix} f_i & f_j \\ f_i' & f_j' \end{vmatrix} = f_if_j' - f_jf_i'$$

is the Wronskian of $f_i$ and $f_j$. The method of constructing a 1-form of Wronskian type is particularly useful in the following situation. An entire function is said to be a *pth power* if it can be represented as a convergent power series of the form $\sum_i a_iX^{pi}$, and a meromorphic function is said to be a $p$th power if it is the quotient of two entire functions of $p$th power.

LEMMA 1. *Let $P(X)$ be a polynomial of degree $n$ divisible by $p$ and $P(0) \neq 0$. Suppose that $P'(X) = m\gamma X^{m-1}$ with $\gamma \neq 0$ and $m \geq 3$ is a positive integer relatively prime to $p$. Then for each $c \neq 0, 1$, $P(f) \not\equiv cP(g)$, for all meromorphic functions $f$ and $g$ which are not pth powers.*

*Proof.* From the given properties of $P(X)$, we have $P(X) = Q(X) + \gamma X^m$ where $Q$ is a $p$th power polynomial with $\deg Q = n$. Let $F_c(X,Y,Z)$ be the homogenization of the polynomial $F_c(X,Y,1) = P(X) - cP(Y)$:

$$F_c(X,Y,Z) = Q(X,Z) - cQ(Y,Z) + \gamma X^m Z^{n-m} - c\gamma Y^m Z^{n-m}$$

where $Q(X,Z)$ denotes the homogenization of $Q(X)$. Hence

$$\begin{aligned}\frac{\partial F_c}{\partial X}(X,Y,Z) &= m\gamma X^{m-1}Z^{n-m},\\ \frac{\partial F_c}{\partial Y}(X,Y,Z) &= -m\gamma Y^{m-1}Z^{n-m},\\ \frac{\partial F_c}{\partial Z}(X,Y,Z) &= (n-m)\gamma Z^{n-m-1}(X^m - cY^m).\end{aligned}$$

The common zeros of the preceding equations are all points with $Z = 0$ and also the point $(0,0,1)$. However the point $(0,0,1)$ is not on the curve $C_c = \{F_c(X,Y,Z) = 0\} \subset \mathbf{P}^2(\mathbf{k})$, $c \neq 1$, for if $P(0) - cP(0) = 0$ and $P(0) \neq 0$ then $c = 1$. We now consider the following rational 1-form, well defined on $\mathbf{P}^2(\mathbf{k})$:

$$\omega := \begin{vmatrix} Y/X & Z/X \\ d(Y/X) & d(Z/X) \end{vmatrix} = \frac{\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}}{X^2}.$$

Rewrite $\omega$ as

$$\omega = X^{m-3}\eta, \qquad \eta = \frac{\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}}{X^{m-1}}. \tag{3.5}$$

Note that $\eta$ is not well defined on $\mathbf{P}^2(\mathbf{k})$ but is a well defined rational 1-form on $\mathbf{k}^3 \setminus \{0\}$. From (3.4) and the expressions above for $\partial F_c/\partial X, \partial F_c/\partial Y$, we see that, on the curve $\pi^{-1}(C_c) \subset \mathbf{k}^3 \setminus \{0\}$ (where $\pi : \mathbf{k}^3 \setminus \{0\} \to \mathbf{P}^2(\mathbf{k})$ is the standard projection):

$$\eta = \frac{\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}}{X^{m-1}} \equiv -\frac{\begin{vmatrix} Z & X \\ dZ & dX \end{vmatrix}}{Y^{m-1}}. \tag{3.6}$$

The LHS of (3.6) is regular except possibly when $X = 0$ (note that the numerator may vanish when $X = 0$); on the other hand the RHS is regular except possibly when $Y = 0$; hence it is regular with the possible exception at $X = Y = 0$. By (3.5), when $m \geq 3$, the same is true for $\omega$. However, as observed earlier, the point $(0,0,1)$ is not in $C_c = \{F_c(X,Y,Z) = 0\}$, $c \neq 1$. Suppose that there exists a non-constant holomorphic map $\phi = [f_0, f_1, f_2]$ : $\mathbf{k} \to C_c \subset \mathbf{P}^2(\mathbf{k})$. Since $f_2 \not\equiv 0$ (otherwise the map is constant) we may represent the map as $\phi = [f = f_0/f_2, g = f_1/f_2, 1]$. The condition $\phi(\mathbf{k}) \subset C_c$ implies that $P(f) - cP(g) \equiv 0$ and $\phi^*\omega \equiv 0$. By the definition of $\omega$ this implies that (using the expression on the LHS of (3.6)) $-g' = W(g,1) \equiv 0$, i.e., $g$ is a $p$th power. Analogously, using the expression on the RHS of (3.6) yields $f' = W(1, f) \equiv 0$, i.e., $f$ is a $p$th power. ■

Note that in the preceding lemma, if $n = m+1$ then the curve $F_c(X, Y) = P(X) - cP(Y)$, $c \neq 0, 1$, is non-singular, and the preceding proof can be simplified by using the classical genus formula. However, for $n > m+1$ the curve is singular and the classical genus formula cannot be applied unless we know that the curve is irreducible. Irreducibility is a condition that is usually very difficult to verify. The Wronskian construction bypasses this difficulty. Next we deal with the curve $F(X, Y) = (P(X) - P(Y))/(X - Y) = 0$. The case of $F(X, Y)$ is more complicated. In the present situation the curve $F(X, Y) = 0$ turns out to be always singular for the class of polynomials $P$ under consideration. As we shall see the Wronskian construction still works provided that we impose one (fairly minor) additional condition (see condition (C3) below) on the polynomial $P$, as counter-examples for uniqueness exist without this condition (see Section 5). The conditions on $P$ in Lemma 1 may be equivalently stated as follows:

$$\text{(C1)} \qquad P(X) = Q(X) + \gamma X^m + b, \qquad \gamma \neq 0,\ b \neq 0,\ 1 \leq m < n,$$

$m$ and $n$ are relatively prime where $Q(X)$ is a $p$th power polynomial:

$$\text{(C2)} \qquad Q(X) = \sum_{l=0}^{q} a_l X^{n_l}, \qquad n_l = p^{\alpha_l} \beta_l,$$

$0 < n_0 < n_1 < \ldots < n_q = n$. Thus the polynomial $F(X, Y)$ is of the form

$$F(X, Y) = \sum_{l=0}^{q} Q_l(X, Y) + \gamma\Big(\sum_{i=0}^{m-1} X^{m-i-1} Y^i\Big) \tag{3.7}$$

where

$$Q_l(X, Y) = a_l (X - Y)^{p^{\alpha_l} - 1} \Big(\sum_{i=0}^{\beta_l - 1} X^{\beta_l - i - 1} Y^i\Big)^{p^{\alpha_l}}.$$

We shall impose an additional condition on the lowest degree term of $Q(X)$:

$$\text{(C3)} \qquad p^{\alpha_0} \beta_0 = n_0 < m.$$

In other words, $\gamma X^m$ is not the term of the lowest degree of the polynomial $P(X) - P(0) = P(X) - b$. Note that the condition (C3) implies that $m \geq 3$.

LEMMA 2. *Let $P(X) = Q(X) + \gamma X^m + b$ be a polynomial of degree $n$ satisfying the conditions of Lemma* 1, *and assume in addition that $m$ is not the lowest degree term of $P(X) - b$. Then $F(f, g) \neq 0$ for all $f, g \in \mathcal{M}^*(\mathbf{k})$ which are not pth powers.*

*Proof.* As remarked prior to the lemma, the conditions on $P$ are equivalent to the conditions (C1), (C2) and (C3). Let $F(X, Y, Z)$ be the homogenization of the polynomial $F(X,Y,1)=F(X,Y)$ (see (3.7)):

$$F(X,Y,Z)=\sum_{l=0}^{q} a_l(X-Y)^{p^{\alpha_l}-1}\Big(\sum_{i=0}^{\beta_l-1} X^{\beta_l-i-1}Y^i\Big)^{p^{\alpha_l}} + \gamma Z^{n-m}\sum_{i=0}^{m-1} X^{m-i-1}Y^i$$

with the gradient

$$\begin{aligned}
\frac{\partial F}{\partial X}(X,Y,Z) &= \frac{m\gamma(X-Y)X^{m-1}Z^{n-m}-F(X,Y,Z)}{(X-Y)^2},\\
\frac{\partial F}{\partial Y}(X,Y,Z) &= \frac{-m\gamma(X-Y)Y^{m-1}Z^{n-m}+F(X,Y,Z)}{(X-Y)^2},\\
\frac{\partial F}{\partial Z}(X,Y,Z) &= -(n-m)\gamma Z^{n-m-1}\sum_{i=0}^{m-1} X^{m-i-1}Y^i.
\end{aligned}$$

On the curve $C=\{F(X,Y,Z)=0\}$ these reduce to

$$\begin{aligned}
\frac{\partial F}{\partial X}(X,Y,Z) &= \frac{m\gamma X^{m-1}Z^{n-m}}{X-Y},\\
\frac{\partial F}{\partial Y}(X,Y,Z) &= \frac{-m\gamma Y^{m-1}Z^{n-m}}{X-Y},\\
\frac{\partial F}{\partial Z}(X,Y,Z) &= m\gamma Z^{n-m-1}\sum_{i=0}^{m-1} X^{m-i-1}Y^i.
\end{aligned}$$

Consider the 1-form

$$\eta := \frac{(X-Y)}{ZX^{m-1}}\begin{vmatrix} Y & Z\\ dY & dZ\end{vmatrix}.$$

Note that $\eta$ is well defined only on $\mathbf{k}^3\setminus\{0\}$. By (3.4) the restriction of $\eta$ to the curve $\pi^{-1}(C)$ where $C=\{F(X,Y,Z)=0\}\subset \mathbf{P}^2(\mathbf{k})$ may also be expressed as

$$\eta := \frac{(X-Y)\begin{vmatrix} Y & Z\\ dY & dZ\end{vmatrix}}{ZX^{m-1}} \equiv -\frac{(X-Y)\begin{vmatrix} Z & X\\ dZ & dX\end{vmatrix}}{ZY^{m-1}} \equiv -\frac{\begin{vmatrix} X & Y\\ dX & dY\end{vmatrix}}{\sum_{i=0}^{m-1} X^{m-i-1}Y^i}. \tag{3.8}$$

The 1-form is well defined only on $\mathbf{k}^3\setminus\{0\}$. As remarked earlier, for any homogeneous polynomial $B$ of degree 2,

$$\varrho = \frac{1}{B}\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}$$

is a well defined rational 1-form on the projective space, hence we may multiply $\varrho$ by any rational function (i.e., quotient of two homogeneous polynomial of the same degree) on the projective space to get a well defined rational 1-form. This means that we need to multiply $\eta$ by a homogeneous polynomial of degree $m-3 \geq 0$ to get a well defined 1-form on the projective space. With this in mind we introduce the following rational 1-form $\omega$ well defined on $\mathbf{P}^2(\mathbf{k})$:

$$\begin{aligned} \omega &:= (X^{\beta_0-1} + X^{\beta_0-2}Y + \ldots + Y^{\beta_0-1})^{p^{\alpha_0}}(X-Y)^{m-3-(\beta_0-1)p^{\alpha_0}}\eta \\ &= \frac{(X^{\beta_0-1} + X^{\beta_0-2}Y + \ldots + Y^{\beta_0-1})^{p^{\alpha_0}}(X-Y)^{m-2-(\beta_0-1)p^{\alpha_0}}}{ZX^{m-1}}\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}. \end{aligned}$$

From (3.8), we see that $\eta$, hence also $\omega$, has no poles except possibly at $(0,0,1)$. Indeed, from the identity

$$\frac{(X-Y)\begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}}{ZX^{m-1}} \equiv -\frac{\begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}}{\sum_{i=0}^{m-1} X^{m-i-1}Y^i}$$

we infer that there is no pole along $Z = 0$, since the points of the curve $C$ at infinity are of the form $\{(1,\nu,0) \mid \nu^n = 1\}$ and the denominator of the LHS does not vanish at such points because $m$ is relatively prime to $n$.

We now check that $\omega$ is regular at $(0,0,1)$. Let $D(0;\varepsilon) := \{u \in \mathbf{k} \mid |u|_v < \varepsilon\}$ be an open disc centered at the origin with radius $\varepsilon > 0$. Let $\psi = (x,y,1)$ be any local analytic map from $D(0;\varepsilon)$ to the curve $C$ such that $\psi(0) = (0,0,1)$. It suffices to show that $\mathrm{ord}_0\,\omega(x,y,1) \geq 0$. By symmetry it is clear that $\mathrm{ord}_0(x) = \mathrm{ord}_0(y) := \mu$. This implies that $\mathrm{ord}_0(x-y) \geq \mu$ and $\mathrm{ord}_0(x^i) = \mathrm{ord}_0(y^i)$ for all $i$, hence

$$\mathrm{ord}_0(Q_l(x,y)) = \mathrm{ord}_0\left((x-y)^{p^{\alpha_l}-1}\Big(\sum_{i=0}^{\beta_l-1} x^{\beta_l-1-i}y^i\Big)^{p^{\alpha_l}}\right) \geq (p^{\alpha_l}\beta_l - 1)\mu$$

for all $l$ and

$$\mathrm{ord}_0\Big(\sum_{i=0}^{m-1} x^{m-1-i}y^i\Big) \geq (m-1)\mu.$$

Since $p^{\alpha_0}\beta_0$ is the lowest degree of the non-constant monomials in the polynomial $P(X)$, we infer that

$$\{(m-1)\mu, \min_{1\leq l\leq q}\{(p^{\alpha_l}\beta_l - 1)\mu\}\} > (p^{\alpha_0}\beta_0 - 1)\mu.$$

On the curve $C = \{F(X,Y,Z) = 0\}$,

$$Q_0(X,Y) = -\sum_{1\le l\le q} Q_l(X,Y) - \gamma \sum_{i=0}^{m-1} X^{m-1-i}Y^i,$$

hence

$$\mathrm{ord}_0(Q_0(x,y)) \ge \min\Big\{\min_{1\le l\le q}\{\mathrm{ord}_0(Q_l(x,y))\}, \mathrm{ord}_0\Big(\sum_{i=0}^{m-1} x^{m-1-i}y^i\Big)\Big\},$$

which is equivalent to

$$\mathrm{ord}_0\Big((x-y)^{p^{\alpha_0}-1}\Big(\sum_{i=0}^{\beta_0-1} x^{\beta_0-1-i}y^i\Big)^{p^{\alpha_0}}\Big) > (p^{\alpha_0}\beta_0 - 1)\mu.$$

This last inequality implies that

$$\mathrm{ord}_0(x-y) > \mu \tag{3.9}$$

or

$$\mathrm{ord}_0\Big(\sum_{i=0}^{\beta_0-1} x^{\beta_0-1-i}y^i\Big) > (\beta_0-1)\mu. \tag{3.10}$$

To estimate the order of $\omega$ at 0 note that $\mathrm{ord}_0\, x' = \mathrm{ord}_0\, x - 1 = \mu - 1$, hence

$$\mathrm{ord}_0 \begin{vmatrix} y & 1 \\ y' & 0 \end{vmatrix} \ge \mu - 1.$$

If (3.9) holds the order of $\omega(x,y,1)$ at 0 is at least

$$\begin{aligned} &p^{\alpha_0}(\beta_0-1)\mu + (m-2-p^{\alpha_0}(\beta_0-1))(\mu+1) + \mu - 1 - (m-1)\,\mu \\ &\qquad = m - \beta_0\, p^{\alpha_0} + p^{\alpha_0} - 3 \ge p^{\alpha_0} - 2 \ge 0. \end{aligned}$$

If (3.10) holds then this order is at least

$$\begin{aligned} &p^{\alpha_0}((\beta_0-1)\mu + 1) + (m-2-p^{\alpha_0}(\beta_0-1))\mu + \mu - 1 - (m-1)\mu \\ &\qquad = p^{\alpha_0} - 1 > 0. \end{aligned}$$

This shows that $\omega$ is regular at $(0,0,1)$. Therefore $\omega$ is regular on $C = \{F(X,Y,Z) = 0\}$.

Suppose that the curve has a component, $C'$, of genus zero; then the restriction of $\omega$ to $C'$, being a regular 1-form, must be identically zero. Since the genus of $C'$ is zero there exists a non-trivial holomorphic map $\phi = [f_0, f_1, f_2] : \mathbf{k} \to C' \subset \mathbf{P}^2(\mathbf{k})$. Since $f_2 \not\equiv 0$ (otherwise the map is constant) we may represent the map as $\phi = [f = f_0/f_2, g = f_1/f_2, 1]$. The condition that $\phi(\mathbf{k}) \subset C'$ implies that $(P(f) - P(g))/(f-g) \equiv 0$ and $\phi^*\omega \equiv 0$. By the definition of $\omega$ this means that either $\phi^*\eta \equiv 0$ or $(f^{\beta_0-1} + f^{\beta_0-2}g + \ldots + g^{\beta_0-1})^{p^{\alpha_0}}(f-g)^{m-3-(\beta_0-1)p^{\alpha_0}} \equiv 0$. The second alternative is eliminated, since $F(X,Y)$ has no linear factor by Proposition 4 and $(X^{\beta_0-1}+X^{\beta_0-2}Y+\ldots+Y^{\beta_0-1})^{p^{\alpha_0}}$ decomposes into linear factors as the field is algebraically closed. The first alternative is eliminated because $\phi^*\eta\equiv 0$ implies that $-g'=W(g,1)\equiv 0$, and $f'=W(1,f)\equiv 0$, i.e., $f$ and $g$ are $p$th powers contrary to the assumption that $f$ is not a $p$th power. ∎

*Proof of Theorem 2.* By Proposition 3 there is no loss of generality in assuming that $\alpha=0$. Suppose that $f$ and $g$ are two non-constant meromorphic functions such that $P(f)=\beta P(g)$ for some constant $\beta\neq 0$. If $f$ and $g$ are not $p$th powers then Lemmas 1 and 2 imply that $\beta=1$ and $f\equiv g$. It remains to deal with the case where $f$ is a $p$th power. Suppose that $f=f_0^{p^i}$, $i\geq 1$, where $f_0$ is not a $p$th power. We claim that $g$ is also a $p$th power. Differentiating the identity $P(f)=\beta P(g)$, using the assumption on $P$, yields

$$\beta g^{m-1}g'=\gamma f^{m-1}f'\equiv 0,$$

which implies that $g$ is also a $p$th power so $g=g_0^{p^l}$ for some $l\geq 1$ and $g_0$ is not a $p$th power. Indeed, $g$ is also a $p^i$th power (i.e., $i=l$). This can be seen by using the expression (1.2) in the introduction:

$$P_S(X)=\sum_{0\leq j\leq n,\, p|j} a_jX^j+aX^m+b.$$

Let $\widehat{a}$, $\widehat{b}$, $\widehat{a}_j$ be chosen such that $\widehat{a}^{p^i}=a$, $\widehat{b}^{p^i}=b$, $\widehat{a}_j^{p^i}=a_j$ and define a polynomial

$$P_0(X)=\sum_{0\leq j\leq n,\, p|j} \widehat{a}_jX^j+\widehat{a}X^m+\widehat{b};$$

then $P_S(f)=P_0(f_0)^{p^i}$. Similarly, $P_S(g)=P_1(g_0)^{p^l}$ where

$$P_1(X)=\sum_{0\leq j\leq n,\, p|j} \widetilde{a}_jX^j+\widetilde{a}X^m+\widetilde{b},$$

and $\widetilde{a}$, $\widetilde{b}$, $\widetilde{a}_j$ are chosen such that $\widetilde{a}^{p^l}=a, \widetilde{b}^{p^l}=b, \widetilde{a}_j^{p^l}=a_j$. Thus $P(f)=\beta P(g)$ implies that $P_0(f_0)^{p^i}=\beta P_1(g_0)^{p^l}$. If $l\leq i$ then $P_0(f_0)^{p^{i-l}}=\gamma P_1(g_0)$, where $\gamma^{p^l}=\beta$, is not a $p$th power by the assumptions on $P_S$ and that $g_0$ is not a $p$th power. This implies that $i=l$ and that $P_0(f_0)=\beta P_0(g_0)$. By construction the polynomial $P_0$ satisfies the assumptions of the theorem, and since $f_0$ and $g_0$ are not $p$th powers we conclude as before that $\beta=1$ and $f_0\equiv g_0$, which, of course, implies that $f\equiv g$. This shows that $P_S$ is a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$. By property (P1) in the introduction $P_S$ is also a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$. Finally property (P3) asserts that this is equivalent to the set $S$ being a unique range set for $\mathcal{A}^*(\mathbf{k})$. ∎

**4. Application of the Truncated Second Main Theorem.** In this section, we will deal with polynomials of the form $P(X) = X^n + aX^m + b$ where $n$ is a power of $p$, $m$ is prime to $n$ and $ab \neq 0$ . This type of polynomial was discussed by Boutabaa, Cherry and Escassut in [2]. However their results do not cover all possible cases of (strong) uniqueness polynomials for $\mathcal{A}^*(\mathbf{k})$ and $\mathcal{M}^*(\mathbf{k})$. The main tool for this is the Truncated Second Main Theorem (see [3]):

THEOREM (Second Main Theorem in positive characteristic). *Let $f = f_1/f_2$ where $f_1, f_2$ are entire functions without common zeros and assume that $f$ is not a pth power. Let $c_1, \ldots, c_q$ be $q$ distinct elements in $\mathbf{k}$. Then*

$$(q-2)\max\{T_{f_1}(t), T_{f_2}(t)\} \leq \sum_{i=1}^{q} N_1(f - c_i, t) - \log t + O(1)$$

*where $N_1(f - c_i, t)$ is the counting function of $f - c_i$, with the number of zeros counted without multiplicity.*

For the case of function fields of positive characteristic the Second Main Theorem for rational functions can be found in [9] and [10].

LEMMA 3. *Let $P(X) = X^n + aX^m + b$, with $m < n = p^r s$, $r, s \geq 1$, $p \nmid s$, $m$ prime to $n$ and $ab \neq 0$. Then*

(i) *$P(X)$ is a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$ if*

$$(n, m) \notin \{(2p^r, 1), (p^r, 1)\} \cup \{(p^r, 2)\} \cup \{(5, 3)\} \cup \{(n, n-1)\},$$

(ii) *$P(X)$ is a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$ if*

$$s \geq 2 \quad \textit{or} \quad s = 1 \quad \textit{and} \quad 3 \leq m \leq n-2.$$

*Proof.* By Proposition 1, to show that $P(X)$ is a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$ (resp. $\mathcal{A}^*(\mathbf{k})$) it suffices to consider $P(f)$ for rational functions $f$ (resp. polynomials). Suppose that $f$ and $g$ are two distinct non-constant rational functions such that $P(f) = P(g)$. As in the proof of Theorem 2 we may assume that neither $f$ nor $g$ is a $p$th power. Next we represent the rational functions as

$$f = \frac{hf_1}{f_2}, \qquad g = \frac{hg_1}{f_2}$$

where $h, f_1, g_1, f_2$ are polynomials such that (1) $f_1$ and $g_1$ are relatively prime (i.e., no common zeros) and (2) $f_2$ is relatively prime to $h$. The condition that $P(f) = P(g)$ is equivalent to

$$h^{n-m}(f_1^s - g_1^s)^{p^r} = -af_2^{n-m}(f_1^m - g_1^m).$$

We now claim that $f_1/g_1$ is not a $p$th power. If it is, then both $f_1$ and $g_1$ have to be $p$th powers since $f_1$ and $g_1$ are relatively prime. Hence the above identity shows that $h/f_2$ is also a $p$th power. This implies that $f = hf_1/f_2$

is also a $p$th power, which contradicts our assumption. Decomposing the above identity into linear factors we get, as $n = p^r s$,

$$h^{p^r s-m}(f_1 - g_1)^{p^r-1}\prod_{i=1}^{s-1}(f_1 - \mu_i g_1)^{p^r} = -af_2^{p^r s-m}\prod_{i=1}^{m-1}(f_1 - \nu_i g_1) \tag{4.1}$$

where $\mu_i, i = 1, \ldots, s-1$ (resp. $\nu_i$, $1 \le i \le m-1$), are the distinct (as $s$ and $m$ are relatively prime to $p$) roots of the polynomials $X^{s-1} + X^{s-2} + \ldots + X + 1$ (resp. $X^{m-1} + X^{m-2} + \ldots + X + 1$). In fact the set $\{1, \mu_1, \ldots, \mu_{s-1}, \nu_1, \ldots, \nu_{m-1}\}$ consists of mutually distinct elements as $m$ is relatively prime to $n = p^r s$. If $\xi$ is a root of $f_1 = g_1$, then since $f_1$ and $g_1$ have no common zero, $f_1(\xi) = g_1(\xi) \neq 0$. This implies, as $\nu_i \neq 1$, that $f_1(\xi) \neq \nu_i g_1(\xi)$ for $i = 1, \ldots, m-1$. Conversely, a root of $f_1 - \nu_i g_1$ is not a root of $f_1 - g_1$ either. For the same reason, as $\mu_i$ and $\nu_j$ are distinct for all $i, j$, $f_1 - \mu_i$ and $f_1 - \nu_j g_1$ have no common roots either. Lastly, by construction, the polynomials $f_2$ and $h$ have no common zeros. Putting all these together we conclude that

$$[h^{p^r s-m} = 0] = \Big[\prod_{i=1}^{m-1}(f_1 - \nu_i g_1) = 0\Big],$$

$$\Big[(f_1 - g_1)^{p^r-1}\prod_{i=1}^{s-1}(f_1 - \mu_i g_1)^{p^r} = 0\Big] = [f_2^{p^r s-m} = 0]$$

where the bracket indicates the divisors of zero counting multiplicity. Consequently, we have

$$\prod_{i=1}^{m-1}(f_1 - \nu_i g_1) = bh^{p^r s-m}$$

for some constant $b$; in particular, $\prod_{i=1}^{m-1}(f_1 - \nu_i g_1)$ is a $(p^r s - m)$th power. As $\nu_i \neq \nu_j$ for $i \neq j$, we conclude that $f_1 - \nu_i g_1$ is a $(p^r s - m)$th power for each $i$ and so

$$N_1\Big(\frac{f_1}{g_1} - \nu_i\Big) \le \frac{1}{p^r s - m} N\Big(\frac{f_1}{g_1} - \nu_i\Big). \tag{4.2}$$

Analogously,

$$(f_1 - g_1)^{p^r-1}\prod_{i=1}^{s-1}(f_1 - \mu_i g_1)^{p^r} = c_1 f_2^{p^r s-m} \tag{4.3}$$

for some constant $c_1$. Again, since $f_1 - g_1$ and $f_1 - \mu_i g_1$ have no common roots we conclude that

$$(p^r - 1)\operatorname{ord}_\xi(f_1 - g_1) = (p^r s - m)\operatorname{ord}_\xi f_2$$

if $\xi$ is a root of $f_1 - g_1$. This implies that

$$N_1\left(\frac{f_1}{g_1} - 1\right) \le \frac{\gcd(p^r s - m, p^r - 1)}{p^r s - m} N\left(\frac{f_1}{g_1} - 1\right) \tag{4.4}$$

provided that $p^r s - m > 0$. Analogously we also have

$$p^r \operatorname{ord}_{\xi_i}(f_1 - \mu_i g_1) = (p^r s - m) \operatorname{ord}_{\xi_i} f_2$$

if $\xi_i$ is a root of $f_1 - \mu_i g_1$. Since $p^r$ and $p^r s - m$ are relatively prime, $\operatorname{ord}_{\xi_i}(f_1 - \mu_i g_1)$ is a multiple of $p^r s - m$ and so

$$N_1\left(\frac{f_1}{g_1} - \mu_i\right) \le \frac{1}{p^r s - m} N\left(\frac{f_1}{g_1} - \mu_i\right) \tag{4.5}$$

provided that $p^r s - m > 0$. The Second Main Theorem, applied to $f_1/g_1$ and $1, \mu_1, \ldots, \mu_{s-1}$, $\nu_1, \ldots, \nu_{m-1}$, yields (by (4.2) and (4.4) and (4.5))

$$\begin{aligned}
&(m + s - 3) \max\{\deg f_1, \deg g_1\} \\
&\quad \le N_1\left(\frac{f_1}{g_1} - 1\right) + \sum_{i=1}^{s-1} N_1\left(\frac{f_1}{g_1} - \mu_i\right) + \sum_{i=1}^{m-1} N_1\left(\frac{f_1}{g_1} - \nu_i\right) - 1 \\
&\quad \le \frac{1}{p^r s - m}\left\{\gamma N\left(\frac{f_1}{g_1} - 1\right) + \sum_{i=1}^{s-1} N\left(\frac{f_1}{g_1} - \mu_i\right) + \sum_{i=1}^{m-1} N\left(\frac{f_1}{g_1} - \nu_i\right)\right\} - 1 \\
&\quad \le \left(\frac{\gamma + m + s - 2}{p^r s - m}\right) \max\{\deg f_1, \deg g_1\} - 1,
\end{aligned}$$

where $\gamma = \gcd(p^r s - m, p^r - 1)$ provided that $p^r s - m > 0$. This implies that

$$(m + s - 3)(p^r s - m - 1) < \gamma + 1 \le p^r s - m + 1, \tag{4.6}$$

which in particular yields

$$(m + s - 4)(p^r s - m - 1) < 2. \tag{4.7}$$

Thus, for $(n, m)$ in the cases:

(1) $m = n - 2 = p^r s - 2,\ m + s \ge 6$, (2) $m \le n - 3 = p^r s - 3,\ m + s \ge 5$,

we have $(m + s - 3)(p^r s - m - 1) \ge 2$ contradicting (4.7). In other words, any $(n, m)$ in cases (1) and (2) yields a uniqueness polynomial.

On the other hand, if $n - m = p^r s - m = 1$ then (4.6) is satisfied, hence $(n, m) = (n, n-1)$ must be excluded. Note that (4.6) is automatically satisfied if $m + s \le 3$ $(m \ge 1, s \ge 1)$, thus $(n, m) = (2p^r, 1), (p^r, 1)$ and $(p^r, 2)$ must also be excluded. To see which other cases should be excluded we need only consider those $(n, m)$ such that $m \le n - 2$ and $m + s \ge 4$. If $m \ge 5$ then $m + s \ge 6$ is automatically satisfied, thus these are not to be excluded (by (1) and (2) above). If $m = 4$, then $n \ne m + 2$ since $m$ and $n$ are relatively prime. Thus, $m \le n - 3$, and in this case, $m + s \ge 5$ is automatically satisfied. These are not to be excluded by (2) above. It remains to consider the case $m \leq 3$ and $m+s=4$. Clearly we have either $m=3, s=1$ or $m=1, s=3$ (the case $m=s=2$ is eliminated by the assumption that $n, m$ are relatively prime). If $m=3, s=1$ it is easily seen that $\gamma = \gcd(p^r-3, p^r-1) \leq 2$. In these cases (4.7) is not useful but we deduce from (4.6) that $0 \leq p^r - 4 = p^r s - m - 1 < \gamma + 1 \leq 3$ and we again arrive at a contradiction, except in the cases $(n,m) = (4,3), (5,3)$. Thus these two cases have to be excluded. If $m=1, s=3$ then the greatest common divisor of $(3p^r-1, p^r-1)$ is again at most 2, hence (4.6) implies that $3p^r - 1 < 3$, which is impossible. Thus none of these are excluded. This completes the proof of (i).

If $f \neq g$ are non-constant polynomials then $f_2 = 1$, hence, by (4.3), $f_1 - g_1$, $f_1 - \mu_i g_1$, $1 \leq i \leq s-1$, are constants. If $s \geq 2$, then this implies that $f_1$ and $g_1$ are constants, contradicting our assumption. Therefore it suffices to consider the case $s=1$. In this case, $f_1 - g_1 = c \neq 1$ is still a constant, and by applying the Second Main Theorem to $f_1/g_1$ and $1, \nu_1, \ldots, \nu_{m-1}$ we get

$$\begin{aligned}
(m-2)\max\{\deg f_1, \deg g_1\} &\leq N_1\left(\frac{f_1}{g_1} - 1\right) + \sum_{i=1}^{m-1} N_1\left(\frac{f_1}{g_1} - \nu_i\right) - 1 \\
&\leq \frac{1}{n-m}\sum_{i=1}^{m-1} N\left(\frac{f_1}{g_1} - \nu_i\right) - 1 \\
&\leq \left(\frac{m-1}{n-m}\right)\max\{\deg f_1, \deg g_1\} - 1.
\end{aligned}$$

This yields

$$\left(m - 2 - \frac{m-1}{n-m}\right)\max\{\deg f_1, \deg g_1\} \leq -1.$$

Clearly, this is impossible if $(m-2)n \geq m^2 - m - 1$. In other words, we derive a contradiction when $m \geq 3$ and

$$n \geq \frac{m^2 - m - 1}{m-2} = m + 1 + \frac{1}{m-2} \geq m+2.$$

This completes the proof of (ii). ∎

Lemma 4. *Let $P(X) = X^n + aX^m + b$, with $m < n = p^r s$, $r, s \geq 1$, $p \nmid s, m$ prime to $n$ and $ab \neq 0$. Then*

(i) *if $s \geq 3$ and $1 \leq m \leq p^r$, then there exist no non-constant $f, g \in \mathcal{M}^*(\mathbf{k})$ such that $P(f) = cP(g)$ for $c \neq 0, 1$;*

(ii) *if $s \geq 2$ or $s = 1$ and $m \geq 3$ then there exist no non-constant $f, g \in \mathcal{A}^*(\mathbf{k})$ such that $P(f) = cP(g)$ for some $c \neq 0, 1$.*

*Proof.* Suppose that there exist non-constant rational functions $f$ and $g$ such that $P(f) = cP(g)$, $c \neq 0, 1$. As in the preceding lemma, we may assume that none of the functions $f, g, f/g$ is a $p$th power. Write $f = f_1/f_2$ and $g = g_1/f_2$ where $f_1$ and $f_2$ (resp. $g_1$ and $f_2$) are polynomials with no common zero. Then $f_1$ and $g_1$ have no common zero, for if $f_1(u) = g_1(u) = 0$ then $b = P(0) = P(f(u)) = cP(g(a)) = cb$, which is impossible since $b \neq 0$ and $c \neq 1$. It is also easy to see from the equation $P(f) = cP(g)$ that $\deg f_1 = \deg g_1 \geq \deg f_2$. From the equation we also derive

$$(f_1^s - \alpha g_1^s)^{p^r} + b(1-c) f_2^{p^r s} = -a(f_1^m - c g_1^m) f_2^{p^r s - m} \tag{4.8}$$

where $\alpha^{p^r} = c$. Since the vanishing order of every zero of the function on the LHS above is a multiple of $p^r$, the identity above implies that the vanishing order of every zero of the function $f_1^m - c g_1^m$, which is not a zero of $f_2$, is a multiple of $p^r$. Suppose that $u$ is a common zero of $f_1^m - c g_1^m$ and $f_2$; then the preceding identity shows that it is also a zero of $f_1^s - \alpha g_1^s$. Thus, as the roots of $f_1^m - c g_1^m$ are distinct ($m$ being prime to $p$), the vanishing order of $f_1^m - c g_1^m$ at $u$ is also a multiple of $p^r$. This implies that $\{-a(f_1^m - c g_1^m) - b(1-c) f_2^m\} f_2^{p^r - m}$ is a $p^r$th power. Rewrite the equation (4.8) as

$$(f_1^s - \alpha g_1^s)^{p^r} = (\{-a(f_1^m - c g_1^m) - b(1-c) f_2^m\} f_2^{p^r - m}) f_2^{p^r(s-1)}; \tag{4.9}$$

this shows that $N_1(f_1^s - \alpha g_1^s) \leq N_1(\{-a(f_1^m - c g_1^m) - b(1-c) f_2^m\} f_2^{p^r - m})$. Apply the Truncated Second Main Theorem to $f_1/g_1$ and $s$ distinct values $\alpha_1, \ldots, \alpha_s$, where $\alpha_i$ is a root of the equation $X^s = \alpha$. We get

$$\begin{aligned}
(s-2) &\max\{\deg f_1, \deg g_1\} \\
&\leq \sum_{i=1}^{s} N_1(f_1/g_1 - \alpha_i) - 1 = \sum_{i=1}^{s} N_1(f_1 - \alpha_i g_1) - 1 \\
&\leq \frac{1}{p^r}((p^r - m) N(f_2) + N(-a f_1^m + a c g_1^m - b(1-c) f_2^m)) - 1 \\
&\leq \frac{1}{p^r}(p^r - m + m) \max\{\deg f_1, \deg g_1\} - 1 \\
&= \max\{\deg f_1, \deg g_1\} - 1
\end{aligned}$$

which is impossible if $s \geq 3$. This completes the proof of (i).

If $f$ and $g$ are polynomials then $f_2 = 1$. In this case, we have

$$(f^s - \alpha g^s)^{p^r} = -a f^m + a c g^m - b(1-c). \tag{4.10}$$

Then $-af^m + acg^m - b(1-c)$ and $f^m - cg^m$ are $p^r$th powers. Apply the Truncated Second Main Theorem to $f_1/g_1$ and $s + m$ distinct values $\alpha_1, \ldots, \alpha_s$, $\beta_1, \ldots, \beta_m$, where $\alpha_i$'s are the roots of the equation $X^s = \alpha$ and $\beta_j$'s are the roots of $X^m = c$. We have

$$\begin{aligned}
(s+m-2)&\max\{\deg f_1, \deg g_1\} \\
&\le \sum_{i=1}^{s} N_1(f/g-\alpha_i) + \sum_{i=1}^{m} N_1(f/g-\beta_j) - 1 \\
&= N_1(-af^m + acg^m - b(1-c)) + N_1(f^m - cg^m) - 1 \\
&\le \frac{1}{p^r}(N(-af^m + acg_1^m - b(1-c)) + N(f^m - cg^m)) - 1 \\
&\le \frac{2m}{p^r}\max\{\deg f_1, \deg g_1\} - 1.
\end{aligned}$$

This yields

$$\left(s - 2 + m\left(1 - \frac{2}{p^r}\right)\right)\max\{\deg f_1, \deg g_1\} \le -1.$$

Clearly, this is impossible if $s \ge 2$. If $s = 1$ and $m \ge 3$ then $p^r \ge 4$. Hence the above inequality is also impossible in this case. This completes the proof of (ii). ■

## 5. Proof of Theorem 3

PROPOSITION 5. *Suppose that $P(X) = X^{p^r} + aX^m + b$ with $r \ge 1$ and $a, b \ne 0$. If $m = 1, 2$ or $p^r - 1$ then $P(X)$ is not a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$.*

*Proof.* For $m = 1$ choose $\alpha$ such that $\alpha^{p^r-1} = -a$. Then $P(X+\alpha) = P(X)$, hence $P(X)$ is not a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$.

If $m = 2$ then $F(X,Y) = (X-Y)^{p^r-1} + a(X+Y)$. The functions

$$f = -\frac{1}{a}\left(\frac{t}{2}\right)^{p^r-1} + \frac{t}{2} \quad \text{and} \quad g = -\frac{1}{a}\left(\frac{t}{2}\right)^{p^r-1} - \frac{t}{2}$$

clearly satisfy the equation $F(f,g) = 0$, hence $P(X)$ is not a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$.

If $m = p^r - 1$ let $Q(X) = a^{-p^r}P(aX) - 1 - ba^{-p^r} = X^{p^r} + X^{p^r-1} + 1$. By Proposition 3, $P(X)$ is a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$ if and only if $Q(X)$ is. Since $Q(X) = Q(X-1)$ the polynomial $Q$ cannot be a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$. ■

PROPOSITION 6. *Suppose that $P(X) = X^n + aX^m + b$ with $a, b \ne 0$. If either $n = 2p^r$, $m = 1$ and $p \ne 2$, or $n = 5$, $m = 3$ and $p = 5$, then $P(X)$ is not a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$.*

*Proof.* If $n = 2p^r$ and $m = 1$ then $F(X,Y) = (X-Y)^{p^r-1}(X+Y)^{p^r} + a$. The functions

$$f = \frac{\alpha}{2}\left(\frac{1}{t^{p^r-1}} + t^{p^r}\right) \quad \text{and} \quad g = \frac{\alpha}{2}\left(\frac{1}{t^{p^r-1}} - t^{p^r}\right),$$

where $\alpha^{2p^r-1} = -a$, satisfy the equation $F(f,g) = 0$. Hence $P(X)$ is not a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$.

For the second case where $n = 5, m = 3$, we take

$$f = \frac{\alpha t(\omega^2 t^2 - \omega)}{(\omega - 1)(t^2 + \omega)^2} \quad \text{and} \quad g = \frac{\alpha t(t^2 - 1)}{(\omega - 1)(t^2 + \omega)^2}$$

where $\omega^2 + \omega + 1 = 0$ and $\alpha^2 = -a$. By a direct calculation we get

$$f - g = \frac{-\alpha\omega^2 t}{t^2 + \omega}, \qquad f - \omega g = \frac{-\alpha\omega t^3}{(t^2 + \omega)^2}, \qquad f - \omega^2 g = \frac{-\alpha\omega t}{(t^2 + \omega)^2}.$$

Hence, $(f - g)^4 = -a(f^2 + fg + g^2)$ and this implies that $P(X)$ is not a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$. ∎

*Proof of Theorem 3.* By Proposition 3, we may assume that $P_S(X) = X^n + aX^m + b$ with $a, b \neq 0$. By Proposition 5, $P_S(X)$ is not a uniqueness polynomial for $\mathcal{A}^*(\mathbf{k})$ if $n = p^r$ and $m = 1$ or $m = 2$ or $m = n - 1$. On the other hand, Lemma 3, Lemma 4 and property (P3) in the introduction imply that $S$ is a unique range set for $\mathcal{A}^*(\mathbf{k})$ if either (a) $n = p^r$ and $3 \le m \le n-2$ or (b) $n = p^r s$, $s > 1$, and $m \ge 1$. This completes the proof of (1).

If $m = n - 1$ then $F(X,Y,Z) = 0$ has only one singular point $(0,0,1)$ which is ordinary and has multiplicity $n-2$. Thus the curve $C = [F(X,Y,Z) = 0]$ is irreducible and its genus is 0. Therefore $P(X)$ is not a uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$. If either $n = 2p^r$, $m = 1$ and $p \neq 2$, or $n = p = 5$ and $m = 3$, then $P(X)$ is not a uniqueness polynomial by Proposition 6. Except in these cases, $P(X)$ is a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{k})$ by Lemmas 1, 3 and 4. ∎

## References


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

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

[3] A. Boutabaa and A. Escassut, *Nevanlinna theory in characteristic p and applications*, preprint.

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

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

[6] W. Cherry and J. T.-Y. Wang, *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.

[7] 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.

[8] 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.

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

[10] —, *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 6.5.2002*
*and in revised form on 6.8.2002* (4282)