BOLETIM
DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

Bol. Soc. Bras. Mat., Vol. 23, Ns. 1–2, 93-108

Linear systems on curves with no Weierstrass points

Masaaki Homma

Abstract. We study order-sequences of linear systems on smooth curves and establish the formula: $b_j + b_{N-j} \leq b_N$ for all j, where $\{b_0 < b_1 < \ldots < b_N\}$ is the order-sequence of a linear system on a curve. As an application of the formula, we describe all linear systems on curves which have no Weierstrass points.

0. Introduction

In the characteristic-free approach to Weierstrass points of a linear system on a curve, we meet the concept of *Weierstrass order-sequences* of a linear system (see, Schmidt [**14, 15**], Matzat [**13**], Laksov [**11, 12**] and Stöhr-Voloch [**16**].)

Let $\mathcal{D}$ be a linear system of projective dimension N on a smooth curve C over an algebraically closed field and let $P \in C$. A nonnegative integer m is a Hermite invariant of $\mathcal{D}$ at P if there is a divisor $D \in \mathcal{D}$ such that the multiplicity of D at P is m. It is obvious that there are $N+1$ Hermite invariants $\{\mu_0(P) < \ldots < \mu_N(P)\}$ of $\mathcal{D}$ at P. A basic result is that there are $N+1$ integers $\{b_0 < \ldots < b_N\}$ such that the Hermite invariants of $\mathcal{D}$ at P coincide with $\{b_0 < \ldots < b_N\}$ for all but finitely many points $P \in C$. This sequence is called the *Weierstrass order-sequence* of $\mathcal{D}$. A point $P \in C$ is a Weierstrass point if $\{\mu_0(P) < \ldots < \mu_N(P)\} \neq \{b_0 < \ldots < b_N\}$. If the characteristic of the ground field is zero, then every Weierstrass order-sequence is classical, that is $b_j = j$ for every j. In positive characteristic p, however, this is not always true. In this case, as Schmidt has shown [**14, Satz 6**], each Weierstrass order-sequence $\{b_0 < \ldots < b_N\}$ has the following property: *if b is a nonnegative integer such that*

$$\binom{b_k}{b} \not\equiv 0 \mod p$$

for some k, then $b = b_j$ for some j. Conversely, as Stöhr and Voloch have shown

Received 2 November 1991.

[16], a sequence of nonnegative integers with this property is the Weierstrass order-sequence of a certain linear system of a curve.

Recently, relations between projective geometry of curves and their Weierstrass order-sequences have been studied by several authors e.g., Ballico-Russo [1], Garcia-Voloch [2], Hefez-Kakuta [3], Hefez-Voloch [4], Homma [6, 7, 8], Homma-Kaji [9], Kaji [10]. In this paper, we prove the following formula on Weierstrass order-sequences.

Theorem I. *If $\{b_0 < \ldots < b_N\}$ is a Weierstrass order-sequence of a linear system on a curve, then we have*

$$b_j + b_{N-j} \leq b_N$$

for all $j = 0, \ldots, N$.

As an application of the formula, we prove the following theorem. A Weierstrass order-sequence $\{b_0 < \ldots < b_N\}$ will be called *symmetric* if the equalities $b_j + b_{N-j} = b_N$ $(j = 0, \ldots, N)$ hold.

Theorem II. *Let C be a smooth curve over an algebraically closed field k and L a line bundle on C. Let V be a nonzero k-subspace of $H^0(C, L)$ and $\mathcal{D} = \mathbb{P}V$ the linear system corresponding to V. Then C has no $\mathcal{D}$-Weierstrass points if and only if $C = \mathbb{P}^1$, the Weierstrass order-sequence $\{b_0 < \ldots < b_N\}$ of $\mathcal{D}$ is symmetric and b_N coincides with the degree of $\mathcal{D}$. In this case, taking suitable coordinates S and T of $\mathbb{P}^1$, V is spanned by $\{S^{b_j}T^{b_{N-j}} \mid j = 0, \ldots, N\}$ in $H^0(\mathbb{P}^1, \mathcal{O}(b_N))$.*

1. Abstract Order-Sequences

Throughout this section, we fix a prime number p.

Let m, n be two nonnegative integers with p-adic expansions:

$$m = \alpha_e p^e + \alpha_{e-1}p^{e-1} + \ldots + \alpha_0 \quad (0 \leq \alpha_i < p)$$
$$n = \beta_e p^e + \beta_{e-1}p^{e-1} + \ldots + \beta_0 \quad (0 \leq \beta_i < p).$$

Then we denote by $m \succ_p n$ (or $n \prec_p m$) if $\alpha_i \geq \beta_i$ for all i. It is easy to show that

$$\binom{m}{n} \not\equiv 0 \mod p$$

if and only if $m \succ_p n$. In this case, we say that m dominates n or m is a dominator for n.

Definition 1.1. An AO (= abstract order)-sequence of dimension N with respect to p is an sequence of $N+1$ nonnegative integers $\{b_0 < b_1 < \cdots < b_N\}$ with the following property: if b is a nonnegative integer such that $b \prec_p b_k$ for some k, then $b = b_j$ for some j. A member of an AO-sequence will be called an *order*.

Note that $b_0 = 0$ by the definition. In particular, the only example of an AO-sequence of dimension 0 is $\{0\}$. Thus, from now on, we assume that $N \geq 1$.

Definition 1.2. An AO-sequence $\{b_0 < b_1 < \ldots < b_N\}$ is said to be of separable type if $b_1 = 1$.

Remark 1.3. If an AO-sequence $\{b_0 < b_1 < \ldots < b_N\}$ is not of separable type, then b_1 is a positive power of p and divides every b_i. In this case,

$$\{b_0(=0) < b_1/b_1(=1) < b_2/b_1 < \ldots < b_N/b_1\}$$

is an AO-sequence of separable type.

Proof. A proof of this fact is an easy exercise. □

Remark 1.4. Let $\mathcal{D}$ be a linear system of projective dimension $N > 0$ on a curve. It is easy to show that if B is the set of base points of $\mathcal{D}$, then $\mathcal{D}$'s Weierstrass order-sequence coincides with $\mathcal{D}(-B)$'s. So every Weierstrass order-sequence is an AO-sequence (cf. **[16, Cor. 1.8]**). When the linear system $\mathcal{D}$ has no base points, the corresponding morphism $\Phi_{\mathcal{D}}: C \to \mathbb{P}^N$ is separable if and only if the Weierstrass order-sequence of $\mathcal{D}$ is of separable type.

Remark 1.5. A sequence of nonnegative integers $\{a_0 < \ldots < a_N\}$ is the Weierstrass order-sequence of a linear system on a curve if and only if it is an AO-sequence.

Proof. See **[16, Remark after Prop. 1.6]**. □

In the rest of this section, we take up several properties of AO-sequences, which will be used in the next section.

Lemma 1.6. *Let $B = \{b_0 < \ldots < b_N\}$ be an AO-sequence. If b_k is a maximal element with respect to the order $\succ_p$ i.e., $b_i \succ_p b_k$ implies $b_i = b_k$, then $B \backslash \{b_k\}$ is also an AO-sequence.*

Proof. Let b' be a nonnegative integer such that $b' \prec_p b_l$ for some $b_l \in B \backslash \{b_k\}$. So we have $b' \in B$. Suppose $b' = b_k$, then $b_l = b_k$ by maximality of b_k, which is a contradiction. So we have $b' \in B \backslash \{b_k\}$. □

Corollary 1.7. *Let $B = \{b_0 < \ldots < b_N\}$ be an AO-sequence and M be any integer such that $0 \leq M \leq N$. Then $\{b_0 < \ldots < b_M\}$ is also an AO-sequence.*

Proof. This is a consequence of Lemma 1.6. □

Corollary 1.8. *Let $B = \{b_0 < \ldots < b_N\}$ be an AO-sequence. For a fixed element b_k, let $D = \{b_i \in B \mid b_i \succ_p b_k\}$. Then $B \backslash D$ is also an AO-sequence.*

Proof. This is also an easy consequence of Lemma 1.6. □

Let m be a nonnegative integer. We denote by $\operatorname{coeff}_{p^i} m$, the coefficient of p^i of the p-adic expansion of m.

Definition 1.9. The *height* of a positive integer m is the maximum in the integers i with $\operatorname{coeff}_{p^i} m \neq 0$. For an AO-sequence $B = \{b_0 < \ldots < b_N\}$, we define the height of B, denoted height B, to be the height of b_N.

Example 1.10. Obviously, if an order b of an AO-sequence is of height 0, then every nonnegative integer less than b is also an order. Therefore, if B is an AO-sequence of dimension N and of height 0, then B coincides with $\{0, 1, \ldots, N\}$.

2. A Basic Formula

The purpose of this section is to prove the following theorem.

Theorem 2.1. *Let $\{b_0 < \ldots < b_N\}$ be a Weierstrass order-sequence of a linear system on a curve. Then we have $b_j + b_{N-j} \leq b_N$ for every $j = 0, \ldots, N$.*

When the characteristic of the ground field is zero, since $b_j = j (j = 0, \ldots, N)$, the assertion is trivial. So we may assume that the characteristic of the ground field is $p > 0$. In this case, as explained before, each Weierstrass order-sequence is an AO-sequence with respect to p. So our theorem is a consequence of the following theorem.

Theorem 2.2. *Let $\{b_0 < \ldots < b_N\}$ be an AO-sequence with respect to a prime number p. Then we have $b_j + b_{N-j} \leq b_N$ for every $j = 0, \ldots, N$.*

We start with an example.

Example 2.3. An AO-sequence $\{b_0 < \ldots < b_N\}$ is said to be *classical* if $b_j = j$ for every $j = 0, \ldots, N$. Obviously, every classical AO-sequence is *symmetric*, that is $b_j + b_{N-j} = b_N$ for every j. In particular, Theorem 2.2 is true for all AO-sequences of height 0 (cf. Example 1.10).

Now we prove Theorem 2.2. Let $\mathcal{A}$ be the family of AO-sequences with respect to p. If $B = \{b_0 < \ldots < b_N\} \in \mathcal{A}$, we define the *index* of B to be $(N, b_N, b_{N-1}, \ldots, b_0)$. We define a total order on $\mathcal{A}$ by the lexicographic order of indices. Obviously, every nonempty subset of $\mathcal{A}$ has the minimum element with respect to the total order.

Suppose that there is an AO-sequence for which the conclusion of Theorem 2.2 does not hold. Let $B = \{b_0 < \ldots < b_N\}$ be the minimum element of the such AO-sequences. By Example 2.3, we have height B (say e) ≥ 1. Let j be the minimum integer such that $b_j + b_{N-j} > b_N$. Note that $j > 0$ because $b_0 + b_N = b_N$ and that $b_j \leq b_{N-j}$ because of the minimality of j. Setting

$$\operatorname{coeff}_{p^e} b_j = \alpha$$
$$\operatorname{coeff}_{p^e} b_{N-j} = \beta$$
$$\operatorname{coeff}_{p^e} b_N = \gamma,$$

we must have $0 \leq \alpha \leq \beta \leq \gamma < p$ and $\gamma \neq 0$.

Claim 1. *If b_k is a maximal element of B with respect to the order $\succ_p$, then we have $k \geq N - j$.*

Proof. By Lemma 1.6, $B \backslash \{b_k\}$ is also an AO-sequence. Suppose $k < N - j$ and put

$$B \backslash \{b_k\} = \{b'_0 < \ldots < b'_{N-1}\}.$$

Then we have $b'_i = b_i$ if $i < k$ and $b'_i = b_{i+1}$ if $i \geq k$, in particular, $b'_j \geq b_j$, $b'_{(N-1)-j} = b_{N-j}$ and $b'_{N-1} = b_N$. Hence we have

$$b'_j + b'_{(N-1)-j} \geq b_j + b_{N-j} > b_N = b'_{N-1}.$$

Hence $B \backslash \{b_k\}$ gives a counter-example to the assertion of Theorem 2.2, which is a contradiction, because $B \backslash \{b_k\}$ is smaller than B with respect to their indices. □

Claim 2. *Let ϵ be an integer such that $0 \leq \epsilon \leq \gamma$. Let*

$$\tilde{B}(\epsilon) := \{b \in B \mid \epsilon p^e \leq b < (\epsilon + 1) p^e\}$$
$$B(\epsilon) := \{b - \epsilon p^e \mid b \in \tilde{B}(\epsilon)\}.$$

Then we have

$$B(0) \supset B(1) \supset \ldots \supset B(\gamma)$$

and each $B(\epsilon)$ forms an AO-sequence.

Proof. First we prove $B(\epsilon) \supset B(\epsilon+1)$ for each ϵ with $0 \le \epsilon \le \gamma - 1$. Let $c \in B(\epsilon+1)$. Since $c < p^e$, we have $(\epsilon+1)p^e + c \succ_p \epsilon p^e + c$. Hence $\epsilon p^e + c \in B$, because $(\epsilon+1)p^e + c \in B$. This means $c \in B(\epsilon)$.

Next we prove that $B(\epsilon)$ forms an AO-sequence. Let c' be a nonnegative integer such that $c' \ {}_{p}\!\!\prec c$ for some $c \in B(\epsilon)$. Since $\epsilon p^e + c \succ_p \epsilon p^e + c'$ and $\epsilon p^e + c \in B$, we have $\epsilon p^e + c' \in B$. So we have $c' \in B(\epsilon)$. □

Claim 3. $B(0) = \ldots = B(\beta)$.

Proof. We may assume that $\beta > 0$. Let $c \in B(0)$. From Claim 1, there is an integer $b \in B$ such that $b \succ_p c$ and $b \ge b_{N-j}$. Letting $\mathrm{coeff}_{p^e} b = \delta$, we have $\delta \ge \beta$ because $b_{N-j} \in \tilde{B}(\beta)$. Writing as $b = \delta p^e + c'$, we have $c' \succ_p c$, because $c < p^e$ and $b \succ_p c$. Hence $\delta p^e + c' \succ_p \beta p^e + c$ and hence $\beta p^e + c \in B$. So $c \in B(\beta)$. Therefore, by Claim 2, we have $B(0) = \ldots = B(\beta)$. □

Claim 4. *Let $B(0) = \{c_0 < c_1 < \ldots < c_n\}$. Then we have*

$$B(0) = \ldots = B(\beta) = \ldots = B(\gamma - 1) \supset B(\gamma)$$

and

$$B(\gamma) = \{c_0 < c_1 < \ldots < c_h\}$$

for some $h \le n$. So we have $\gamma(n+1) + h = N$.

Proof. The last assertion is a consequence of the preceding assertion because

$$N = {}^{\#}B - 1 = \sum_{\epsilon=0}^{\gamma} {}^{\#}B(\epsilon) - 1.$$

To prove the first assertion, we may assume that $B(0) \supsetneqq B(\gamma)$. Let δ be the minimum integer such that $B(0) \supsetneqq B(\delta)$. Note that $\delta > \beta$ by Claim 3. For each integer ϵ such that $\delta \le \epsilon \le \gamma$, put

$$\tilde{B}_+(\epsilon) := \{\epsilon p^e + c \mid c \in B(0)\}.$$

Obviously,

$$B_+ := B(0) \cup \tilde{B}(1) \cup \ldots \cup \tilde{B}(\delta - 1) \cup \tilde{B}_+(\delta) \cup \ldots \cup \tilde{B}_+(\gamma)$$

is also an AO-sequence. Note that $B_+ \supset B$ and the first successive $\delta(n+1)$ elements of B_+ are contained in B. Let $B' = \{b'_0 < b'_1 < \ldots < b'_N\}$ be the first successive $N+1$ integers of B_+. From Corollary 1.7, B' is an AO-sequence. Since $\delta > \beta$, we have $b'_j = b_j$, $b'_{N-j} = b_{N-j}$ and $b'_N \le b_N$. Hence we have

$$b'_j + b'_{N-j} = b_j + b_{N-j} > b_N \ge b'_N,$$

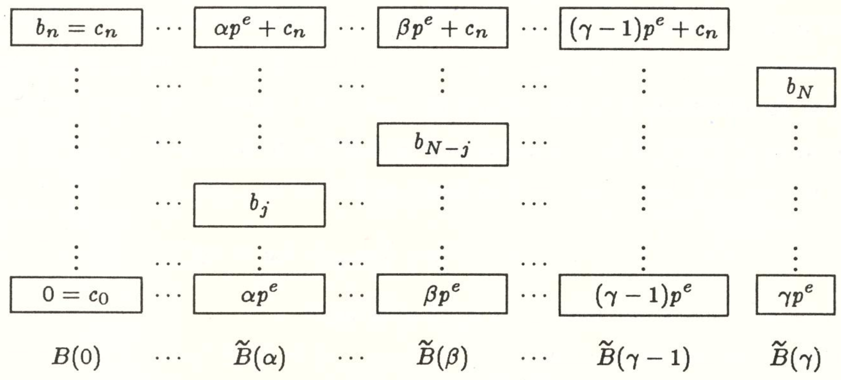
which means B' is a counter-example to the conclusion of Theorem 2.2. Since B is the minimum member of among all counter-examples and B' is smaller than or equal to B with respect to the total order of $\mathcal{A}$, B must coincides with B'. □

By Claim 4,

$$b_N = \gamma p^e + c_h$$

and there are integers f, g with $0 \le f, g \le n$ such that

$$b_{N-j} = \beta p^e + c_g$$
$$b_j = \alpha p^e + c_f.$$



Claim 5. $\alpha = \beta = 0$ *and* $\gamma = 1$.

Proof. Since

$$j = {}^{\#}\{b \in B \mid b > b_{N-j}\} = h + 1 + (\gamma - 1 - \beta)(n+1) + (n - g)$$

and

$$j = {}^{\#}\{b \in B \mid b < b_j\} = \alpha(n+1) + f,$$

we have

$$h + 1 + (n-g) + (\gamma - \beta - 1)(n+1) = f + \alpha(n+1). \tag{1}$$

Since $n - g \ge 0$ and $f < n+1$, (1) implies

$$(\gamma - \beta - 1)(n+1) \le f + \alpha(n+1) < (\alpha+1)(n+1).$$

Hence we have

$$\gamma \le \alpha + \beta + 1. \tag{2}$$

Similarly, since $n - g < n + 1$ and $h \le n$, (1) implies

$$\alpha + \beta \le \gamma. \tag{3}$$

From (2) and (3), $\gamma = \alpha + \beta$ or $\alpha + \beta + 1$.

First we consider the case $\gamma = \alpha + \beta$. Substituting $\alpha + \beta$ for γ in the equation (1), we have

$$h + 1 + (n - g) + (\alpha - 1)(n + 1) = f + \alpha(n + 1).$$

So we have $h = f + g$. On the other hand, since

$$(\alpha + \beta)p^e + c_f + c_g = b_j + b_{N-j} > b_N = \gamma p^e + c_h$$

and $\gamma = \alpha + \beta$, we have $c_f + c_g > c_h$. Those mean $\{c_0 < c_1 < \ldots < c_h\}$, which is an AO-sequence because of Claim 2, is a counter-example to Theorem 2.1. Since the height of the AO-sequence is less than e, that contradicts the choice of B as the minimum member among all counter-examples. Therefore γ must be equal to $\alpha + \beta + 1$. Substituting $\alpha + \beta + 1$ for γ in the equation (1), we have $(n + 1) + h = f + g$. On the other hand, since

$$(\alpha + \beta)p^e + c_f + c_g = b_j + b_{N-j} > b_N = \gamma p^e + c_h$$

and $\gamma = \alpha + \beta + 1$, we have $c_f + c_g > p^e + c_h$.

Now, consider the sequence

$$B' = \{c_0 < c_1 < \ldots < c_n < p^e + c_0 < \ldots < p^e + c_h\}.$$

Obviously, B' is an AO-sequence of height e and of dimension $n + h + 1$. Writing as $B' = \{b'_0 < b'_1 < \ldots < b'_{n+h+1}\}$, we have $b'_i = c_i$ if $i \leq n$ and $b'_{n+i} = p^e + c_{i-1}$. Since $n + h + 1 - f = g$ and $c_f + c_g > p^e + c_h$, we have

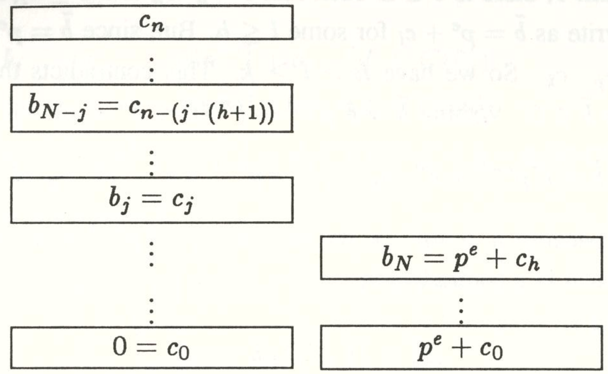
$$b'_f + b'_{(n+h+1)-f} = c_f + c_g > p^e + c_h = b'_{n+h+1}.$$

This means B' is also a counter-example to the conclusion of Theorem 2.2. Since $B' \subset B$, we have $B' = B$ by the minimality of B. In particular, we have $\alpha = \beta = 0$ and $\gamma = 1$. □

By the previous Claims, our situation was reduced to the following: There is an AO-sequence $C = \{c_0 < c_1 < \ldots < c_n\}$ of height $< e$ such that

$$\begin{aligned} B &= \{b_0 < \ldots < b_N\} \\ &= \{c_0 < c_1 < \ldots < c_n < p^e + c_0 < \ldots < p^e + c_h\} \end{aligned}$$

for some $h \leq n$ and $b_j, b_{N-j} \in B(0) = C$. Note that $N = n + h + 1$ and $h + 1 \leq j$ (because $b_{N-j} \in C$).



Claim 6. $e \geq 2$.

Proof. Suppose that $e = 1$. Then since C is of height 0, $C = \{0, 1, \ldots, n\}$ and $n < p$. Hence $b_j = c_j = j$ and $b_{N-j} = c_{n-(j-(h+1))} = n + h + 1 - j$. Since $n < p$, we get $b_j + b_{N-j} = n + h + 1 \leq p + h = b_N$, which is absurd. □

Setting

$$\mathrm{coeff}_{p^{e-1}}\, b_j = \alpha'$$
$$\mathrm{coeff}_{p^{e-1}}\, b_{N-j} = \beta'$$

we must have $0 \leq \alpha' \leq \beta' < p$.

Let ϵ' be an integer such that $0 \leq \epsilon' \leq p - 1$ and let

$$\tilde{C}(\epsilon') := \{c \in C \mid \epsilon' p^{e-1} \leq c < (\epsilon' + 1)p^{e-1}\}$$
$$C(\epsilon') := \{c - \epsilon' p^{e-1} \mid c \in \tilde{C}(\epsilon')\}.$$

Then, by arguments similar to those in the proof of Claim 2, we can show that

$$C(0) \supset C(1) \supset \ldots \supset C(p - 1)$$

and each $C(\epsilon')$ is an AO-sequence.

Claim 7. $C(0) = \ldots = C(\beta')$.

Proof. Suppose that there is an order $d \in C(0)$ such that $d \notin C(\beta')$. Let $D_d := \{b \in B \mid b \succ_p d\}$.

First we show that if $b \in D_d$, then $b \leq c_h$ or $p^e \leq b$. Suppose the contrary: let $c_k \in C$ such that $c_k \succ_p d$ and $c_h < c_k$. Writing as $c_k = \epsilon' p^{e-1} + \epsilon''$, we get $\epsilon'' \succ_p d$ because $d < p^{e-1}$. If $\epsilon' \geq \beta'$, then $c_k \succ_p \beta' p^{e-1} + d$ and then $\beta' p^{e-1} + d \in C$. Hence $d \in C(\beta')$, which is a contradiction. So $\epsilon' < \beta'$. In particular, $c_k < b_{N-j}$ because

$$c_k = \epsilon' p^{e-1} + \epsilon'' < \beta' p^{e-1} \leq b_{N-j}.$$

Hence, by Claim 1, there is $\tilde{b} \in B$ such that $\tilde{b} \succ_p c_k$ and $\tilde{b} \geq b_{N-j}$. If $\tilde{b} \geq p^e$, then we can write as $\tilde{b} = p^e + c_l$ for some $l \leq h$. But, since $\tilde{b} = p^e + c_l \succ_p c_k$, we have $c_l \succ_p c_k$. So we have $h \geq l \geq k$. This contradicts the assumption $c_h < c_k$. Thus $\tilde{b} \in C$. Writing $\tilde{b} = \delta' p^{e-1} + \delta''$ $(0 \leq \delta'' < p^{e-1})$, since

$$\tilde{b} = \delta' p^{e-1} + \delta'' \succ_p c_k = \epsilon' p^{e-1} + \epsilon'', \quad \epsilon'' \succ_p d$$

and $\delta' \geq \beta'$ (because $\tilde{b} \geq b_{N-j}$), we have $\tilde{b} \succ_p \beta' p^{e-1} + d$. Hence we get $d \in C(\beta')$, which is a contradiction.

Now letting

$$D_d^0 = \{b \in D_d | b \leq c_h\}$$
$$D_d^+ = \{b \in D_d | p^e \leq b\},$$

by the preceding remark D_d is the disjoint union of D_d^0 and D_d^+. Moreover, for each $c_k (0 \leq k \leq h)$, $c_k \in D_d^0$ if and only if $p^e + c_k \in D_d^+$. So we have $^\# D_d^0 = {}^\# D_d^+ = \frac{1}{2} {}^\# D_d$. We consider the sequence $B \backslash D_d$, which is an AO-sequence by Corollary 1.8. Put $B \backslash D_d = \{b'_0 < \ldots < b'_{N'}\}$. Then we have $b_j = b'_{j - \# D_d^0}$ and $b_{N-j} = b'_{N' - (j - \# D_d^0)}$ because $b_{N-j} = b'_{N-j-\# D_d^0}$ and $N' = N - {}^\# D_d = N - 2^\# D_d^0$. Since

$$b'_{j-\# D_d^0} + b'_{N'-(j-\# D_d^0)} = b_j + b_{N-j} > b_N \geq b'_{N'} \ ,$$

the AO-sequence $B \backslash D_d$ is also a counter-example to the conclusion of Theorem 2.2. Since B is the minimum member among all counter-examples, we can conclude that $D_d = \emptyset$. □

Let us write as $C(0) = \{d_0 < d_1 < \ldots < d_r\}$.

Claim 8. $C(0) = \ldots = C(\beta') = \ldots = C(p-1)$.

Proof. For each integer ϵ' such that $0 \leq \epsilon' \leq p-1$, let

$$\tilde{C}_+(\epsilon') = \{\epsilon' p^{e-1} + d_\mu | \mu = 0, 1, \ldots, r\}.$$

Then $\tilde{C}_+(0) \cup \ldots \cup \tilde{C}_+(p-1) \cup \{p^e + c_0, \ p^e + c_1, \ldots, p^e + c_h\}$ is an AO-sequence. Let $B' = \{b'_0 < \ldots < b'_N\}$ be the AO-sequence which consists of the first successive $N+1$ integers in the above sequence. Since $\tilde{C}_+(\epsilon') = \tilde{C}(\epsilon')$ for all ϵ' with $0 \leq \epsilon' \leq \beta'$ by Claim 7, we get $b'_j = b_j$ and $b'_{N-j} = b_{N-j}$. Hence B' is also a counter-example to Theorem 2.2. So B must coincides with B'. □

End of Proof. From Claim 8, we can write as

$$\begin{aligned} b_j &= \alpha' p^{e-1} + d_s \quad (d_s \in C(0)) \\ b_{N-j} &= \beta' p^{e-1} + d_t \quad (d_t \in C(0)) \\ b_N &= p^e + \gamma' p^{e-1} + d_u \quad (0 \leq \gamma' < p, \ d_u \in C(0)). \end{aligned}$$

Note that, by Claim 8,

$$B = \left(\bigcup_{\epsilon'=0}^{p-1} \{\epsilon' p^{e-1} + d_\mu | d_\mu \in C(0)\} \right) \cup \left(\bigcup_{\epsilon'=0}^{\gamma'-1} \{p^e + \epsilon' p^{e-1} + d_\mu | d_\mu \in C(0)\} \right) \cup \{p^e + \gamma' p^{e-1} + d_\mu | \ 0 \leq \mu \leq u\}.$$

Since

$$\begin{aligned} j &= {}^\#\{b \in B | b > b_{N-j} (= \beta' p^{e-1} + d_t)\} \\ &= (u+1) + \gamma'(r+1) + (p-1-\beta')(r+1) + r - t \end{aligned}$$

and

$$\begin{aligned} j &= {}^\#\{b \in B | b < b_j (= \alpha' p^{e-1} + d_s)\} \\ &= \alpha'(r+1) + s, \end{aligned}$$

we have

$$(p - 1 - \beta' + \gamma')(r+1) + u + 1 + r - t = \alpha'(r+1) + s. \tag{4}$$

Since $u + 1 + r - t > 0$ and $s < r + 1$, (4) implies

$$(p - 1 - \beta' + \gamma')(r+1) < (\alpha' + 1)(r+1).$$

Hence we have

$$p + \gamma' \leq \alpha' + \beta' + 1. \tag{5}$$

Similarly, since $u + 1 \leq r + 1$ and $r - t \leq r$, (4) implies

$$\alpha' + \beta' \leq p + \gamma'. \tag{6}$$

From (5) and (6), we get $\gamma' = \alpha' + \beta' - p$ or $\alpha' + \beta' + 1 - p$.

Case 1. First we consider the case $\gamma' = \alpha' + \beta' - p$. From (4), we get $u = s + t$. On the other hand, since

$$b_j + b_{N-j} = (\alpha' + \beta') p^{e-1} + d_s + d_t = p^e + \gamma' p^{e-1} + d_s + d_t,$$

$b_N = p^e + \gamma' p^{e-1} + d_u$ and $b_j + b_{N-j} > b_N$, we obtain $d_s + d_t > d_u$. This means that the AO-sequence $\{d_0 < \ldots < d_u\}$ is also a counter-example to Theorem 2.2. But the AO-sequence is of height $< e$, which contradicts the minimality of B.

Case 2. Next we consider the case $\gamma' = \alpha' + \beta' + 1 - p$. By the same argument used in the first case, we have $u + (r+1) = s + t$ and $d_s + d_t > p^{e-1} + d_u$, which mean the AO-sequence

$$\{d_0 < \ldots < d_r < p^{e-1} + d_0 < \ldots < p^{e-1} + d_u\}$$

is also a counter-example. This is a contradiction because the height of the sequence is $e - 1$ ($< e$). So we can conclude that Theorem 2.2 is true for every AO-sequence.

3. Proof of Theorem II

Now we prove Theorem II stated in Introduction. Our proof is divided into two parts.

Theorem 3.1. *Let $\mathcal{D}$ be a linear system on a smooth curve C of degree $d > 0$ and of (projective) dimension $N > 0$ and let $\{b_0 < \ldots < b_N\}$ be the Weierstrass order-sequence of $\mathcal{D}$. Then C has no $\mathcal{D}$-Weierstrass points if and only if $C = \mathbb{P}^1$, $b_N = d$ and $b_j + b_{N-j} = b_N$ for all $j = 0, 1, \ldots, N$.*

Proof. Let W be the ramification divisor of $\mathcal{D}$ (see [12] or [16]; in the terminology of [12], W is the highest Wronskian of $\mathcal{D}$). The divisor W has the following properties:

(i) W is effective of degree

$$(b_0 + \ldots + b_N)(2g-2) + (N+1)d,$$

where g is the genus of C;

(ii) A point $P \in C$ is a $\mathcal{D}$-Weierstrass point if and only if $P \in \operatorname{Supp} W$.

Therefore, C has no $\mathcal{D}$-Weierstrass points if and only if

$$(b_0 + \ldots + b_N)(2-2g) = (N+1)d. \tag{7}$$

If the equation (7) holds, then $g = 0$ because $g > 0$ implies $(N+1)d \leq 0$, which is absurd. Hence our condition is equivalent to

$$\begin{cases} g = 0 \\ 2(b_0 + \ldots + b_N) = (N+1)d. \end{cases} \tag{8}$$

On the other hand, using the fact: $b_N \leq d$ and the inequality proved in Theorem 2.1, we have

$$2(b_0 + \ldots + b_N) \leq (N+1)b_N \leq (N+1)d \tag{9}$$

and all the equalities in (9) hold if and only if $b_N = d$ and $b_j + b_{N-j} = b_N$ for any $j = 0, \ldots, N$. This completes the proof. □

The second step is to prove the following lemma.

Lemma 3.2. *Let V be an $(N+1)$-dimensional subspace of $H^0(\mathbb{P}^1, \mathcal{O}(d))$ and $\{\mu_0 < \ldots < \mu_N\}$ a sequence of nonnegative integers (not necessary an AO-sequence) such that $\mu_N = d$ and $\mu_j + \mu_{N-j} = \mu_N$ ($j = 0, \ldots, N$). Suppose that there are two points $P_1, P_2 \in \mathbb{P}^1$ such that the Hermite invariants of $\mathcal{D} = \mathbb{P}(V)$ at $P_i (i = 1, 2)$ coincides with $\{\mu_0 < \ldots < \mu_N\}$. Then, taking suitable coordinates S, T of $\mathbb{P}^1$, the $N+1$ elements*

$$S^{\mu_0}T^{\mu_N}, S^{\mu_1}T^{\mu_{N-1}}, \ldots, S^{\mu_N}T^{\mu_0}$$

forms a basis of V.

Proof. Choose coordinates S and T of $\mathbb{P}^1$ such that $P_1 = 0 = (0{:}1)$, $P_2 = \infty = (1{:}0)$ and put $s = \dfrac{S}{T}$. Now we consider the isomorphism

$$H^0(\mathbb{P}^1,\ \mathcal{O}(d)) \xrightarrow{\sim} \mathcal{L}(d\infty)$$
$$S^k T^{d-k} \mapsto s^k,$$

where

$$\mathcal{L}(d\infty) = \{f \in k(\mathbb{P}^1) \mid \operatorname{div} f + d\infty \succ 0\} \cup \{0\}.$$

We denote by $\mathcal{L}(\mathcal{D}, d\infty)$, the image of V under the isomorphism. To prove our assertion, it suffices to show that $\mathcal{L}(\mathcal{D}, d\infty)$ is generated by $\{s^{\mu_0}, s^{\mu_1}, \ldots, s^{\mu_N}\}$. Since the Hermite invariants of $\mathcal{D}$ at P_1 are $\{\mu_0 < \ldots < \mu_N\}$, we can choose a basis $\varphi_0, \ldots, \varphi_N$ of $\mathcal{L}(\mathcal{D}, d\infty)$ such that

$$\begin{cases} \varphi_0 = s^{\mu_0} + \sum_{i=\mu_0+1}^{\mu_N} a_{0,i}s^i \\ \quad\vdots \\ \varphi_\alpha = s^{\mu_\alpha} + \sum_{i=\mu_\alpha+1}^{\mu_N} a_{\alpha,i}s^i \\ \quad\vdots \\ \varphi_N = s^{\mu_N}. \end{cases} \tag{10}$$

Furthermore, replacing $\varphi_0, \dots, \varphi_N$ by

$$\begin{aligned}
\varphi'_N &= \varphi_N \\
\varphi'_{N-1} &= \varphi_{N-1} - a_{N-1,\mu_N}\varphi'_N \\
&\vdots \\
\varphi'_\alpha &= \varphi_\alpha - (a_{\alpha,\mu_N}\varphi'_N + \dots + a_{\alpha,\mu_{\alpha+1}}\varphi'_{\alpha+1}) \\
&\vdots \\
\varphi'_0 &= \varphi_0 - (a_{0,\mu_N}\varphi'_N + \dots\dots + a_{0,\mu_1}\varphi'_1),
\end{aligned}$$

we may assume that

$$a_{\alpha,\mu_k} = 0 \quad (k = \alpha+1, \dots, N) \quad \text{for any} \quad \alpha \quad \text{in (10).} \qquad (11)$$

We show that $\varphi_\alpha = s^{\mu_\alpha}$ $(\alpha = 0, \dots, N)$ under the assumption (11). Suppose the contrary. For a number α such that $\varphi_\alpha \neq s^{\mu_\alpha}$, let β be the maximum number such that $a_{\alpha,\beta} \neq 0$. Put $t = \dfrac{T}{S}$ and consider the isomorphism

$$\begin{gathered}
H^0(\mathbb{P}^1, \mathcal{O}(d)) \xrightarrow{\sim} \mathcal{L}(d \cdot 0) \\
S^k T^{d-k} \mapsto t^{d-k}.
\end{gathered}$$

Denoting by $\mathcal{L}(\mathcal{D}, d\cdot 0)$ the image of V under the isomorphism, we get the isomorphism from $\mathcal{L}(\mathcal{D}, d\infty)$ to $\mathcal{L}(\mathcal{D}, d\cdot 0)$ via V. The isomorphism send φ_α to

$$t^{\mu_N} \cdot \varphi_\alpha\left(\frac{1}{t}\right) = t^{\mu_N - \mu_\alpha} + \dots + a_{\alpha,\beta} t^{\mu_N - \beta}.$$

Since t is a local parameter at ∞ and $a_{\alpha,\beta} \neq 0$, $\mu_N - \beta$ must be a Hermite invariant of $\mathcal{D}$ at ∞. Hence we have $\mu_N - \beta = \mu_\gamma$ for some γ. Since $\mu_j + \mu_{N-j} = \mu_N$ for all j, we have $\beta = \mu_{N-\gamma}$, which contradicts (11). This completes the proof.

Addendum. (This note was added in December, 1991). Recently, two nice papers concerning Theorem I have appeared. The first one is

A. Garcia, *Some arithmetic properties of order-sequences of algebraic curves* (Preprint, Oct. 1991) in which he has given a short proof of this theorem. The second one is

E. Esteves, *A geometric proof of an inequality of order sequences* (preprint, Oct. 1991), in which he has given a geometric proof of a generalization of

Theorem I.

Added in proof

Recently, the author found a very short proof of Theorem 1 and another proof of Esteve's generalization which was mentioned in Addendum. The proofs are, however, rather tricky. We will discuss them in another paper.

Acknowledgement

I would like to express my hearty thanks to the referee for his useful comments, and to Professor S. Kleiman for his advice and hospitality during my stay at MIT.

References

1. Ballico, E. and Russo, B., *On the general osculating flag to a projective curve in characteristic p.* preprint 1991.
2. Garcia, A. and Voloch, J.F., *Duality for projective curves.* Bol. Soc. Bras. Mat. 21 (1991), 159-175.
3. Hefez, A. and Kakuta, N., *On the geometry of non-classical curves.* preprint 1991.
4. Hefez, A. and Voloch, J.F., *Frobenius con-classic curves.* Arch. Math. 54 (1990), 263-273.
5. Homma, M., *Funny plane curves in characteristic $p > 0$.* Comm. Alg. 15 (1987), 1469-1501.
6. Homma, M., *Reflexivity of tangent varieties associated with a curve.* Ann. Mat. Pura Appl. (4) 156 (1990), 195-210.
7. Homma, M., *Duality of space curves and their tangent surfaces in characteristic $p > 0$.* Ark. Math. 29 (1991), 221-235.
8. Homma, M., *Space curves with degenerate strict duals.* Comm. Alg. 20 (1992), 867-874.
9. Homma, M. and Kaji, H., *On the inseparable degree of the Gauss map of higher order for space curves.* Proc. Japan Acad. 68, Ser. A (1992), 11-14.
10. Kaji. H., *Strangeness of higher order for space curves.* Comm. Alg. 20 (1992), 1535-1584.
11. Laksov, D., *Weierstrass points on curves.* Astérisque 87/88 (1981), 221-247.
12. Laksov, D., *Wronskian and Plücker formulas for linear systems on curves.* Ann. Sci. École Norm. Sup. (4) 17 (1984), 45-66.
13. Matsat, H. B., *Über Weierstrsspunkte von Fermatkörpern.* Dissertation, Universität Karlsruhe 1972.
14. Schmidt, F.K., *Die Wronskisch Determinante in belebigen differenzierbaren Funktionenkörpern.* Math. Z. 45 (1939), 62-74.

15. Schmidt, F.K., *Zur arithmetischen Theorie der algebraischen Funktionen II: Allgemeine Theorie der Weierstrass punkte.* Math. Z. 45 (1939), 75-96.

16. Stöhr, K.O. and Voloch, J.F., *Weierstrass points and curves over finite fields.* Proc. London Math. Soc. (3) 52 (1986), 1-19.

Masaaki Homma
Department of Mathematics
Faculty of Education
Yamaguchi University
Yamaguchi, 753 Japan

and

Department of Mathematics
MIT
Cambridge, Mass. 02139