Suzuki, J.
Osaka J. Math.
44 (2007), 187–196

MIURA CONJECTURE ON AFFINE CURVES

JOE SUZUKI

(Received June 23, 2005, revised May 10, 2006)

Abstract

Shinji Miura gave certain multivariable polynomials that express an Affine curve for a given algebraic function field F and its degree one place $\mathcal{O}$, if F contains such an $\mathcal{O}$. Suppose the equations contain t (≥ 2) variables, and that the pole orders at $\mathcal{O}$ are $a_1, \ldots, a_t \geq 1$, where $\mathrm{GCD}\{a_1, \ldots, a_t\} = 1$. If

$$\frac{a_i}{d_i} \in \frac{a_1}{d_{i-1}}\mathbb{N} + \cdots + \frac{a_{i-1}}{d_{i-1}}\mathbb{N}, \quad d_i = \mathrm{GCD}\{a_1, \ldots, a_i\}$$

for each $i = 2, \ldots, t$, by arranging $a_1, \ldots, a_t$, then we say that the orders $a_1, \ldots, a_t$ are telescopic. On the other hand, the number t' ($\geq t - 1$) of the equations in the Miura canonical form is determined by $a_1, \ldots, a_t$. If $t' = t - 1$, then we say that $a_1, \ldots, a_t$ are complete intersection. It is known that the telescopic condition implies the complete intersection condition. However, the converse was open thus far. This paper solves the conjecture in the affirmative by giving its proof.

1. Introduction

Let F/K be a function field with degree one place $\mathcal{O}$, and $a_1, \ldots, a_t \geq 1$ ($\mathrm{GCD}\{a_1, \ldots, a_t\} = 1$) generators of the monoid $\{-v_{\mathcal{O}}(f) \geq 0 \mid f \in F\}$ (the non-negative pole orders at $\mathcal{O}$), i.e.

$$a_1\mathbb{N} + \cdots + a_t\mathbb{N} = \{-v_{\mathcal{O}}(f) \geq 0 \mid f \in F\}.$$

Shinji Miura [1, 2] gave generators of the ideal expressing an Affine curve with the point $\mathcal{O}$ at infinity. For $x_1, \ldots, x_t \in F$ such that $a_i = -v_{\mathcal{O}}(x_i)$, the Miura canonical form (MCF) is the set of equations in the form

$$x_1^{M_1} \cdots x_t^{M_t} + \alpha_L x_1^{L_1} \cdots x_t^{L_t} + \sum_{(N_1,\ldots,N_t)\in\mathbb{N}^t} \alpha_N x_1^{N_1} \cdots x_t^{N_t} = 0 \tag{1}$$

with $M = (M_1, \ldots, M_t) \in \mathbb{N}^t$ and $L = (L_1, \ldots, L_t) \in \mathbb{N}^t$, where $\alpha_L, \alpha_N \in K$, $\alpha_L \neq 0$, and

$$\sum_{i=1}^{t} a_i M_i = \sum_{i=1}^{t} a_i L_i > \sum_{i=1}^{t} a_i N_i$$

for $N = (N_1, \ldots, N_t) \in \mathbb{N}^t$, $N \neq L, M$.

2000 Mathematics Subject Classification. Primary 14Q05; Secondary 13A15.

We consider two conditions on $a_1, \ldots, a_t$: telescopic and complete intersection conditions. If

$$\frac{a_i}{d_i} \in \frac{a_1}{d_{i-1}}\mathbb{N} + \cdots + \frac{a_{i-1}}{d_{i-1}}\mathbb{N}, \quad d_i = \mathrm{GCD}\{a_1, \ldots, a_i\}$$

for each $i = 2, \ldots, t$, by replacing $a_1, \ldots, a_t$ with $a_{\sigma(1)}, \ldots, a_{\sigma(t)}$ for some permutation σ in $\{1, \ldots, t\}$, then we say that the orders $a_1, \ldots, a_t$ are telescopic. Notice that the number t' $(\geq t-1)$ of equations contained in the MCF only depends on $a_1, \ldots, a_t$. If $t' = t-1$, then we say that $a_1, \ldots, a_t$ are complete intersection. Miura himself proved that the telescopic condition implies the complete intersection condition. However, the converse was open:

Conjecture 1. *The complete intersection condition implies the telescopic condition.*

In general, the set of polynomials in the form of (1) with arbitrary $a_1, \ldots, a_t$ $(\mathrm{GCD}\{a_1, \ldots, a_t\} = 1)$ and $\alpha_L, \alpha_N \in K$ does not always express a curve. It is required to be a Gröbner basis, which is not easy to recognize by computation. On the other hand, Miura derived that the telescopic condition is sufficient for a MCF to express a curve [1, 2].

This paper solves Conjecture 1 in the affirmative, which means that a complete intersection MCF expresses a curve:

Theorem 1. *The complete intersection condition implies the telescopic condition.*

Section 2 explains basic materials on one-variable algebraic function fields and states the main theorem in Miura theory. Section 3 relates Miura theory in terms of Gröbner base. Section 4 gives a proof of the conjecture.

Throughout the paper, $\mathbb{Z}$, $\mathbb{Z}_+$, $\mathbb{N}$, and $K = \mathbb{F}_q$ denote the integers, the positive integers, the nonnegative integers, the finite field with q elements, respectively.

2. One-variable algebraic function field

If F is a finite algebraic extension of $K(x)$ for some $x \in F$ which is transcendental over a field K, F/K is said to be an algebraic function field of one variable over K. A ring $\mathcal{O}$ such that

1. $K \subset \mathcal{O} \subset F$, $\mathcal{O} \neq K, F$
2. $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$ for any $z \in F$

is said to be a valuation ring of F/K (I.1.4 [5]). Each $\mathcal{O}$ is a local ring, and the maximal ideal $P = \mathcal{O} \setminus \mathcal{O}^*$ is said to be a place, where $\mathcal{O}^* := \{z \in \mathcal{O} \mid z^{-1} \in \mathcal{O}\}$. Hereafter, $\mathbb{P}_F$ denotes the set of places in F/K. Then, for each $P \in \mathbb{P}_F$, $\mathcal{O}_P := \{z \in F \mid z^{-1} \notin P\}$ is a valuation ring of F/K. Furthermore, P is a principal ideal of $\mathcal{O}_P$,

and when we write each $0 \neq z \in F$ by $z = t^n u$ ($u \in \mathcal{O}_P^*$, $n \in \mathbb{Z}$) using $t \in F$ such that $P = t\mathcal{O}_P$, the value of n (the discrete valuation of z at P) does not depend on the choice of t (I.1.6 [5]), and we write it by $v_P(z)$. Let ∞ be the symbol not in $\mathbb{Z}$ such that $\infty + \infty = \infty + n = n + \infty = \infty$ and $\infty > m$ for all $m, n \in \mathbb{Z}$, and let $v_P(0) = \infty$. Then, $v_P : F \to \mathbb{Z} \cup \{\infty\}$ satisfies

1. $v_P(x) = \infty \Longleftrightarrow x = 0$
2. $v_P(xy) = v_P(x) + v_P(y)$, for any $x, y \in F$
3. $v_P(x + y) \geq \min\{v_P(x), v_P(y)\}$, for any $x, y \in F$
4. there exists $z \in F$ such that $v_P(z) = 1$
5. $v_P(a) = 0$, for any $0 \neq a \in K$.

For example, $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$, $\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\}$, $P = \{z \in F \mid v_P(z) > 0\}$ (I.1.12 [5]). Let $F_P := \mathcal{O}_P / P$ and $\deg P := [F_P : K]$.

Assumption 1. *There exists* $P \in \mathbb{P}_F$ *such that* $\deg P = 1$.

Under Assumption 1, the constant field K coincides with

$$\tilde{K} := \{z \in F \mid z \text{ is algebraic over } K\}$$

(we say K to be the full constant field of F). In fact, since $\tilde{K}$ is embedded into F_P via the residue class map $\mathcal{O}_P \to F_P$ (I.1.5 [5]), so $\deg P = 1$ means

$$K = F_P \supseteq \tilde{K} \supseteq K.$$

Hereafter, we arbitrarily fix such $P \in \mathbb{P}_F$ with $\deg P = 1$. We define

$$\mathcal{L}(\infty P) := \{z \in F \mid v_Q(z) \geq 0,\ Q \in \mathbb{P}_F \setminus \{P\}\} \cup \{0\} = \bigcap_{Q \in \mathbb{P}_F \setminus \{P\}} \mathcal{O}_Q$$

and $M_P(R) := \{-v_P(x) \mid x \in R \setminus \{0\}\}$ for integral R such that $K \subset R \subseteq \mathcal{L}(\infty P)$, $K \neq R$. Since an arbitrary monoid in $\mathbb{N}$ is finitely generated, we write the generators of $M_P(R)$ by $a_1, a_2, \ldots, a_t \in \mathbb{Z}_+$, $t \in \mathbb{Z}_+$ and express $A_t = (a_1, \ldots, a_t) \in \mathbb{Z}_+^t$, where the order of $a_1, a_2, \ldots, a_t$ is fixed. If we fix $x_1, x_2, \ldots, x_t \in R \setminus K$ so that $-v_P(x_i) = a_i$, $i = 1, 2, \ldots, t$, then we have $R = K[x_1, x_2, \ldots, x_t]$. Furthermore, let $K[X] := K[X_1, X_2, \ldots, X_t]$ be the the polynomial ring over K of t-variables $X_1, X_2, \ldots, X_t$, and let $\Theta : K[X] \to R$ be the canonical surjective homomorphism from $K[X]$ to R such that for $f(X_1, X_2, \ldots, X_t) \in K[X]$, $\Theta(f(X_1, X_2, \ldots, X_t)) := f(x_1, x_2, \ldots, x_t) \in R$. Then, $\ker \Theta$ makes an ideal in $K[X]$ and from the homomorphism theorem, we have $K[X]/\ker \Theta \simeq R$.

Lemma 1. *The following three are equivalent*:

1. *F is a fraction field of R.*
2. *$\mathbb{N} \setminus M_P(R)$ is a finite set.*

3. $\mathrm{GCD}\{A_t\} = 1$.

(See Miura [1] for proof.)

We choose R so that F is a fraction field of R. Therefore, we have $\mathrm{GCD}\{A_t\} = 1$. Moreover, since the transcendental dimension of F/K is 1, $\ker\Theta$ is an ideal expressing a curve.

We define the map $\Psi : \mathbb{N}^t \to \langle A_t \rangle$ by $\Psi((n_1, \ldots, n_t)) := \sum_i a_i n_i$, and define the order $<$ in $\mathbb{N}^t$ so that $M < M'$ for $M = (m_1, m_2, \ldots, m_t)$ and $M' = (m'_1, m'_2, \ldots, m'_t)$ if
1. $\Psi(M) < \Psi(M')$
2. $\Psi(M) = \Psi(M')$ and $m_1 = m'_1, m_2 = m'_2, \ldots, m_{i-1} = m'_{i-1}$, $m_i > m'_i$ for some i $(1 \le i \le t)$.

Let $M(a)$ be the minimum element with respect to the order $<$ in $\mathbb{N}^t$ satisfying $\Psi(M) = a \in \langle A_t \rangle$. We define $B(A_t) \in \mathbb{N}^t$ and $V(A_t) \subseteq \mathbb{N}^t \setminus B(A_t)$ by

$$B(A_t) := \{M(a) \mid a \in \langle A_t \rangle\}$$

and

$$V(A_t) := \{L \in \mathbb{N}^t \setminus B(A_t) \mid L = M + N,\ M \in \mathbb{N}^t \setminus B(A_t),\ N \in \mathbb{N}^t \Longrightarrow N = (0, 0, \ldots, 0)\},$$

respectively. Also, let

$$T(A_t) := B(A_t) \cap \{(n_1, n_2, \ldots, n_t) \in \mathbb{N}^t \mid n_1 = 0\}.$$

Then, we have

Lemma 2 (Miura [1]).

$$V(A_t) + \mathbb{N}^t = \mathbb{N}^t \setminus B(A_t)$$

and

Lemma 3 (Miura [1]).

$$\#\, T(A_t) = a_1.$$

(See Appendix for proofs.)

Hereafter, for $A \subset K[X]$, $\mathrm{Span}\{A\}$ and (A) denote the linear space over K generated by A and the ideal in $K[X]$ generated by A, respectively. Also, X^M, $M = (m_1, m_2, \ldots, m_t) \in \mathbb{N}^t$, denotes $X^M = X_1^{m_1} X_2^{m_2} \cdots X_t^{m_t}$ for simplicity.

Theorem 2 (Miura [1]). *There exists a set of generators,* $\{F_M \mid M \in V(A_t)\}$, *of* $\ker\Theta \subseteq K[X]$ *satisfying*

C1 *For each* $M \in V(A_t)$,

$$F_M - X^M \in \mathrm{Span}\left\{X^N \mid N \in B(A_t),\ \Psi(N) \le \Psi(M)\right\} \setminus \mathrm{Span}\left\{X^N \mid N \in B(A_t),\ \Psi(N) < \Psi(M)\right\},$$

and

C2 $\mathrm{Span}\{X^N \mid N \in B(A_t)\} \cap (\{F_M \mid M \in V(A_t)\}) = \{0\}$.

C1 is precisely expressed by

$$F_M = X^M + \alpha_L X^L + \sum_{\{N \in B(A_t) \mid \Psi(N) < \Psi(M)\}} \alpha_N X^N, \quad 0 \neq \alpha_L,\ \alpha_N \in K, \tag{2}$$

where $\Psi(M) = \Psi(L)$.

Theorem 3 (Miura [1]). *Suppose we fix* $t \in \mathbb{Z}_+$, $A_t = (a_1, a_2, \ldots, a_t) \in \mathbb{Z}_+^t$, g.c.d$\{A_t\} = 1$. *If* $\{F_M \mid M \in V(A_t)\} \in K[X]$ *satisfies* C1 *and* C2 *in* Theorem 1, *then* $I := (\{F_M \mid M \in V(A_t)\})$ *makes a prime ideal in* $K[X]$. *Moreover, the fraction field of the integral domain* $K[X]/I$ *is a one-variable algebraic function field over* K.

3. Gröbner base

For $f = \sum a_N X^N \in K[X]$, $a_N \in K$, $N \in \mathbb{N}^t$, we define

$$\mathrm{multideg}(f) = \begin{cases} -\infty, & f = 0 \\ \max\{N \in \mathbb{N}^t \mid a_N \neq 0\}, & f \neq 0 \end{cases},$$

where "max" is the maximum in the sense of the order $<$ that has been already defined. We set

$$LT(f) = \begin{cases} 0, & f = 0 \\ a_T X^T, & f \neq 0 \end{cases},$$

where $T := \mathrm{multideg}(f)$. If a finite subset $G = \{G_1, \ldots, G_m\}$ of ideal I satisfies

$$(\{LT(f) \mid f \in I\}) = (\{LT(G_1), \ldots, LT(G_m)\}),$$

G is said to make a Gröbner basis of ideal I with respect $<$. It is known that for any ideal ($\neq \{0\}$) and any order, there exists a Gröbner basis [4].

For ideal I in $K[X]$, we define the Δ-set of I by

$$\Delta(I) = \mathbb{N}^t \setminus \bigcup_{f \in I \setminus \{0\}} \{\mathrm{multideg}(f) + \mathbb{N}^t\}.$$

Proposition 1 (Miura [1]). *Assuming* (2),
1. C2 *is equivalent to that* $\{F_M \mid M \in V(A_t)\} \subseteq K[X]$ *is a Gröbner basis of* $(\{F_M \mid M \in V(A_t)\}) \subseteq K[X]$ *with respect to the order* $<$
2. $\Delta(I) = B(A_t)$.

Therefore, the verification of C2 is not easy except for specific cases.

Lemma 4. *If a basis* $G = \{G_1, \ldots, G_m\}$ *of ideal* I *satisfies* $\mathrm{LCM}(LT(G_i), LT(G_j)) = LT(G_i)LT(G_j)$, $i \neq j$, *then* G *makes a Gröbner basis of* I.

(See [4] for proof.)

Noting the following lemma, we define $SV(A_t) \subseteq V(A_t) \subseteq \mathbb{N}^t \setminus B(A_t)$ by $SV(A_t) := \{N_i \mid 2 \leq i \leq t\}$, where N_i, $2 \leq i \leq t$ is the unique N_i such that $\{N_i\} = \{0\}^{i-1} \times \mathbb{N} \times \{0\}^{t-i} \cap V(A_t)$.

Lemma 5 (Miura [1]). *For each* $2 \leq i \leq t$, *the set* $\{0\}^{i-1} \times \mathbb{N} \times \{0\}^{t-i} \cap V(A_t)$ *has one element.*

If $V(A_t) = SV(A_t)$, i.e. elements of $(\{F_M | M \in V(A_t)\})$ are generated by exactly $t-1$ elements in $K[X]$ (A_t is said to be complete intersection), then $\{F_M \mid M \in V(A_t)\} \subseteq K[X]$ makes a Gröbner basis, so that we do not have to verify C2. In fact, applying $\mathrm{LCM}(LT(F_M), LT(F_N)) = X^M X^N = LT(F_M)LT(F_N)$, $M \in \{0\}^{i-1} \times \mathbb{N} \times \{0\}^{t-i}$, $N \in \{0\}^{j-1} \times \mathbb{N} \times \{0\}^{t-j}$, $2 \leq i < j \leq t$ to Lemma 4, we obtain the claim.

Even if we replace C2 by the complete intersection condition, we do not know how to construct A_t such that $V(A_t) = SV(A_t)$. However, we can construct some A_t such that $V(A_t) = SV(A_t)$ as follows.

DEFINITION 1 (Kirfel-Pellikan [3]). If $A_t = (a_1, \ldots, a_t) \in \mathbb{Z}_+^t$ satisfies

$$\frac{a_i}{d_i} \in \left\langle \frac{a_1}{d_{i-1}}, \ldots, \frac{a_{i-1}}{d_{i-1}} \right\rangle, \quad d_i = \mathrm{GCD}(a_1, \ldots, a_i),\ 1 \leq i \leq t,\ d_0 = 1,$$

then A_t is said to be strictly telescopic. Moreover, A_t is said to be telescopic if A_t becomes strictly telescopic by changing the order of elements in A_t.

Whether A_t is strictly telescopic depends on the order of elements in A_t as well as elements in A_t. If $t = 2$, then $a_2 / \mathrm{GCD}\{a_1, a_2\} \in \langle (1) \rangle$ and A_t is automatically telescopic.

REMARK 1. If $2g - 1 \notin \langle A_t \rangle$, where $g := \#(\mathbb{N} \setminus \langle A_t \rangle)$, A_t is said to be symmetric. The following implication [6] is known:

$$t = 2 \Longrightarrow A_t : \text{telescopic} \Longrightarrow A_t : \text{symmetric}.$$

Proposition 2 (Miura [1]). *If A_t is telescopic, then*

$$SV(A_t) = V(A_t) = \left\{ \left(0, \ldots, 0, \frac{d_{i-1}}{d_i}, 0, \ldots, 0 \right) \;\middle|\; 2 \le i \le t \right\}.$$

Hence, if $t = 2$ (C_{ab}), or if A_t is telescopic, then A_t is complete intersection, so that we do not have to verify C2. However, the converse has been open, i.e. if A_t being complete intersection implies A_t being telescopic. If this is solved in the affirmative, arbitrary complete intersection A_t will be obtained constructively. If we pull back the ideal $I = (\{F_2, \ldots, F_t\})$ in $K[X]$ to the projective space, only $I^* \supseteq (\{F_2^*, \ldots, F_t^*\})$ holds in general. Besides, not all algebraic curves are expressed by complete intersection A_t. However, if we obtain all the expressions with $t-1$ equations relating t variables in MCFs via telescopic A_t, it will be pleasing to engineers who are engaged in algebraic coding theory and algebraic curve cryptography.

Conjecture 2 (Miura [1]). *If A_t is complete intersection, then A_t is telescopic. In other words,*

$$A_t : \textit{telescopic} \iff A_t : \textit{complete intersection.}$$

4. Proof of Miura conjecture

Since we assume $V(A_t) = SV(A_t)$, we may write

$$V(A_t) = \{M^{(2)}, M^{(3)}, \ldots, M^{(t)}\}$$

with

$$M^{(i)} = (0, \ldots, M_i, 0, \ldots, 0), \quad M_i \ge 1,\ i = 2, 3, \ldots, t,$$

and $L^{(i)} := (L_1^{(i)}, \ldots, L_t^{(i)})$ for L corresponding to $M = M^{(i)}$ in (2).

Lemma 6. *There is no $\{i_1, i_2, \ldots, i_k\} \subseteq \{2, 3, \ldots, t\}$ $(1 \le k \le t-1)$ such that*

$$L_{i_1}^{(i_2)} \ge 1, L_{i_2}^{(i_3)} \ge 1, \ldots, L_{i_{k-1}}^{(i_k)} \ge 1, L_{i_k}^{(i_1)} \ge 1. \tag{3}$$

Proof. Suppose there exists a sequence of length k satisfying (3). Let $N := (N_1, \ldots, N_t) \in \mathbb{N}^t$ be such that

$$N_l := \begin{cases} 1, & l \in \{i_1, \ldots, i_k\} \\ 0, & l \notin \{i_1, \ldots, i_k\} \end{cases}.$$

Then, for $M := \sum_{j=1}^{k} M^{(i_j)} - N$ and $L := \sum_{j=1}^{k} L^{(i_j)} - N$, we have $M, L \in \mathbb{N}^t$.

In general, for $H, H' \in \mathbb{N}^t$ such that $\Psi(H) = \Psi(H')$ and $H > H'$, and arbitrary $H'' \in \mathbb{N}^t$, we have

$$\Psi(H + H'') = \Psi(H' + H''), \quad H + H'' > H' + H'',$$

and if $H - H'', H' - H'' \in \mathbb{N}^t$, then

$$\Psi(H - H'') = \Psi(H' - H''), \quad H - H'' > H' - H''.$$

Since $M^{(i)} \notin B(A_t)$ and $L^{(i)} \in B(A_t)$, we have $M^{(i)} > L^{(i)}$, $i = 2, 3, \ldots, t$, so that $\Psi(M) = \Psi(L)$ and $M > L$. Hence, $M \in \mathbb{N}^t \setminus B(A_t)$. On the other hand, since $M = \sum_{j=1}^{k} M^{(i_j)} - N \notin M^{(i)} + \mathbb{N}^t$, $i = 2, 3, \ldots, t$, we have $M \notin V(A_t) + \mathbb{N}^t$. These contradict to Lemma 2. □

We define a partial order $\prec$ in $C = \{2, \ldots, t\}$ as follows:

1. for each $i \in C$: $i = i$
2. for each of two different $i, j \in C$ such that $L_i^{(j)} \geq 1$: $i \prec j$; and
3. for each of three different $i, j, k \in C$ such that $i \prec j$ and $j \prec k$: $i \prec k$.

Also, we fix a total order in C that is consistent with the partial order $\prec$ (such an order exists from Lemma 6), and write the total order by $\prec$ also. Without loss of generality, we may assume $2 \prec 3 \prec \cdots \prec t$ by changing the indices in $M_j, a_j, \{L_i^{(j)}\}_{i=1}^{t}$, $j = 2, 3, \ldots, t$. From Lemma 6, we have

$$M_j a_j = \sum_{i=1}^{j-1} L_i^{(j)} a_i. \tag{4}$$

Lemma 7. *For each $j = 2, \ldots, t$, the ratio d_{j-1}/d_j divides M_j.*

Proof. The right of (4) can be divided by both a_j and d_{j-1}, and therefore can be divided by $a_j d_{j-1}/\mathrm{GCD}(a_j, d_{j-1}) = a_j d_{j-1}/d_j$. Hence, d_{j-1}/d_j divides M_j. □

Lemma 8. $M_2 M_3 \cdots M_t = a_1$

Proof. From Lemma 2, we have

$$B(A_t) = \{(l_1, l_2, \ldots, l_t) \mid l_1 \in \mathbb{N},\ 0 \leq l_j \leq M_j - 1,\ j = 2, 3, \ldots, t\}$$
$$T(A_t) = \{(0, l_2, \ldots, l_t) \mid 0 \leq l_j \leq M_j - 1,\ j = 2, 3, \ldots, t\}.$$

Also, from Lemma 3, we have $M_2 M_3 \cdots M_t = a_1$. □

Theorem 4. *A_t is telescopic if and only if A_t is complete intersection.*

Proof. From $\prod_{j=2}^{t}(d_{j-1}/d_j) = a_1$ and Lemmas 7 and 8, we obtain $M_j = d_{j-1}/d_j$. Hence, (4) is written as

$$\frac{a_j}{d_j} = \sum_{i=1}^{j-1} L_i^{(j)} \frac{a_i}{d_{j-1}}. \tag{5}$$

□

Appendix: Proofs of Lemmas 2 and 3

The following proofs of Lemma 2 and $\#T(A_t) = a_1$ appeared in Miura [1]. We give them here for self-containedness.

Proof of Lemma 2. First, we show

$$(\mathbb{N}^t \setminus B(A_t)) + \mathbb{N}^t = \mathbb{N}^t \setminus B(A_t). \tag{6}$$

$(\mathbb{N}^t \setminus B(A_t)) + \mathbb{N}^t \supseteq \mathbb{N}^t \setminus B(A_t)$ is apparent. On the other hand,

$$\begin{aligned}
&M \notin B(A_t), \quad N \in \mathbb{N}^t \\
&\Longrightarrow \exists M' \in B(A_t) \quad \text{s.t.} \quad M > M', \quad \Psi(M) = \Psi(M'), \quad N \in \mathbb{N}^t \\
&\Longrightarrow M + N > M' + N, \quad \Psi(M+N) = \Psi(M'+N) \\
&\Longrightarrow M + N \notin B(A_t).
\end{aligned}$$

Therefore, (6) holds.

Secondly, From $V(A_t) \subseteq \mathbb{N}^t \setminus B(A_t)$ and (6), we have

$$V(A_t) + \mathbb{N}^t \subseteq \mathbb{N}^t \setminus B(A_t). \tag{7}$$

We derive contradiction, assuming that the inclusion in (7) is not $\subseteq$ but $\subset$. Notice

$$\begin{aligned}
&\exists M_1 \quad \text{s.t.} \quad M_1 \in \mathbb{N}^t \setminus B(A_t), \quad M_1 \notin V(A_t) + \mathbb{N}^t \\
&\Longrightarrow \exists N_1, M_2 \quad \text{s.t.} \quad M_1 = M_2 + N_1, \quad M_2 \in \mathbb{N}^t \setminus B(A_t), \quad (0, 0, \ldots, 0) \neq N_1 \in \mathbb{N}^t \\
&\Longrightarrow \exists M_2 \quad \text{s.t.} \quad M_2 \in \mathbb{N}^t \setminus B(A_t), \quad M_2 \notin V(A_t) + \mathbb{N}^t \\
&\Longrightarrow \exists N_2, M_3 \quad \text{s.t.} \quad M_2 = M_3 + N_2, \quad M_3 \in \mathbb{N}^t \setminus B(A_t), \quad (0, 0, \ldots, 0) \neq N_2 \in \mathbb{N}^t \\
&\Longrightarrow \exists M_3 \quad \text{s.t.} \quad M_3 \in \mathbb{N}^t \setminus B(A_t), \quad M_3 \notin V(A_t) + \mathbb{N}^t \\
&\Longrightarrow \cdots .
\end{aligned}$$

However, this implies an infinite sequence $M_1, M_2, \ldots$, such that $\Psi(M_1) > \Psi(M_2) > \cdots$, which is a contradiction. Therefore, M_1 such that $M_1 \in \mathbb{N}^t \setminus B(A_t)$, $M_1 \notin V(A_t) + \mathbb{N}^t$ does not exist. Hence, the equality holds in (7). □

Proof of Lemma 3. For each $i = 0, 1, \ldots, a_1 - 1$, we define

$$b_i := \min\{b \in \langle a_2, a_3, \ldots, a_t\rangle \mid b \equiv i \bmod a_1\}.$$

We show $|T(A_t)| = a_1$ by deriving $T(A_t) = \{M(b_i) \in B(A_t) \mid i = 0, 1, \ldots, a_1 - 1\}$.

Since $a_1 > 0$ and $\mathrm{GCD}\{A_t\} = 1$, for each $i = 0, 1, \ldots, a_1 - 1$, $\{b \in \langle (a_2, a_3, \ldots, a_t)\rangle \mid b \equiv i \bmod a_1\}$ is not empty.

Let $M, N \in \mathbb{N}^t$ be such that $\Psi(M) > \Psi(N)$ and $\Psi(M) - \Psi(N) = na_1$ for some $n \in \mathbb{Z}_+$. We claim $M \notin T(A_t)$. Let $N' := (n, 0, \ldots, 0) + N$. Since $n > 0$, $N' \notin \{0\} \times \mathbb{N}^{t-1}$ and $\Psi(M) = \Psi(N')$. If $M \notin \{0\} \times \mathbb{N}^{t-1}$, then $M \notin T(A_t)$. If $M \in \{0\} \times \mathbb{N}^{t-1}$, then $\Psi(M) = \Psi(N')$ and $M > N'$, which means $M \notin B(A_t)$. In any case, $M \notin T(A_t)$.

We claim $M(b_i) \in \{0\} \times \mathbb{N}^{t-1}$. To this end, we derive a contradiction, assuming $m_1 \neq 0$ in $M(b_i) = (m_1, m_2, \ldots, m_t)$. Since $\Psi((0, m_2, \ldots, m_t)) + m_1 a_1 = b_i$ and

$$\Psi((0, m_2, \ldots, m_t)) \equiv b_i \equiv i \bmod a_1,$$

$m_1 \neq 0$ implies $\Psi((0, m_2, \ldots, m_t)) < b_i$, which contradicts the minimality of b_i. □

ACKNOWLEDGEMENT. The author sincerely thanks Prof. Sinji Miura for his suggestions.

References

[1] S. Miura: *Error-Correcting Codes based on Algebraic Geometry*, Ph. D. Thesis, University of Tokyo, 1998
[2] S. Miura and N. Kamiya: *Geometric-Goppa codes on some maximal curves and their minimum distance*; in Proc. 1993 IEEE Information Theory Workshop, Shizuoka Japan, June 4–8, 1993, 85–86.
[3] C. Kirfel and R. Pellikan: *The minimum distance of codes in an array coming from telescopic semigroups*, Journal AAECC (1993), 1720–1732
[4] D. Cox, J. Little and D.O'Shea: Ideals, Varieties, and Algorithms, UTM, Springer-Verlag, Berlin, 1992.
[5] H. Stichtenoth: Algebraic Function Fields and Codes, Springer-Verlag, 1993.
[6] A. Nijenhuis and H.S. Wilf: *Representations of integers by linear forms in nonnegative integers*, J. Number Theory **4** (1972), 98–106.

Department of Mathematics
Osaka University
1–1 Machikaneyama, Toyonaka
Osaka 560–0043
Japan
e-mail: suzuki@math.sci.osaka-u.ac.jp