On construction and generalization of algebraic geometry codes[*]

Ryutaroh Matsumoto[†]
Department of Electrical and Electronic Engineering,
Tokyo Institute of Technology, 152-8552 Japan
Email: ryutaroh@ss.titech.ac.jp

and

Shinji Miura
SONY Corporation
Information and Network Technologies Laboratories
Japan
Email: miura@av.crl.sony.co.jp

March 4, 2000

Abstract

The construction, estimation of minimum distance, and decoding algorithms of algebraic geometry codes can be explained without using advanced mathematics by the notion of weight domains. We clarify the relation between algebraic geometry codes and linear codes from weight domains. Then we review a systematic construction which yields all weight domains.

1 Introduction

Algebraic geometry codes were defined in an algebraic geometric way, and many facts about them, in particular estimation of minimum distance and decoding algorithms, are also stated and proved algebraic geometrically. So it had been difficult to understand algebraic geometry codes without the theory of algebraic curves. Recently Høholdt et al. [HvLP97, HvLP98] observed that definition, estimation of minimum distance, and decoding algorithms of algebraic geometry codes could be explained using only the notion of a weight function, which is essentially a discrete valuation, and made understanding of algebraic geometry codes much easier. First we survey the construction of linear codes with weight functions.

[*] This paper appeared in the Proceedings of Algebraic Geometry, Number Theory, Coding Theory and Cryptography, University of Tokyo, Tokyo, Japan, January 19–20, 2000 (ed. T. Katsura et al.), pp. 3–15. The proceedings was published July 2000.

[†] He is supported by JSPS Research Fellowships for Young Scientists.

Linear codes obtained with weight functions are generalization of so-called one-point algebraic geometry codes. Next we survey a characterization of linear codes from weight functions and their comparison to the ordinary one-point AG codes.

We construct linear codes from a commutative ring equipped with a weight function, which we call a weight domain. Finally we survey a systematic construction which yields all weight domains.

We omit proofs of assertions and refer the reader to appropriate literatures when they are available in English.

2 Evaluation codes and weight functions

2.1 Definition of evaluation codes

Throughout this paper K denotes a fixed finite field, and $\mathbf{N}_0$ the set of nonnegative integers. R denotes a commutative K-algebra, and n a positive integer in this section.

Definition 2.1 [HvLP98, Definition 3.5] *A function $\rho : R \to \mathbf{N}_0 \cup \{-\infty\}$ is said to be a* weight function on R *if*

1. *$\rho(f) = -\infty$ iff $f = 0$.*
2. *$\rho(cf) = \rho(f)$ for all nonzero $c \in K$.*
3. *$\rho(f+g) \le \max\{\rho(f), \rho(g)\}$ and the equality holds if $\rho(f) \ne \rho(g)$.*
4. *If $\rho(f) = \rho(g) \ne -\infty$, then there exists $c \in K$ such that $\rho(f - cg) < \rho(g)$.*
5. *$\rho(fg) = \rho(f) + \rho(g)$, where the sum of an integer and $-\infty$ is $-\infty$.*

Remark 2.2 *A weight function is a generalization of the degree of univariate polynomials.*

If R is a K-algebra with a weight function ρ, then there exists a K-basis $\{f_1, f_2, \ldots\}$ such that $\rho(f_i) < \rho(f_{i+1})$ for all i [HvLP98, Proposition 3.12]. We regard the set K^n consisting of n-tuples of elements in K as a commutative ring with the componentwise addition and multiplication. Let $\varphi : R \to K^n$ be an epimorphism of K-algebras. For a positive integer ℓ, we define the *evaluation code* $E_\ell \subset K^n$ by the linear space spanned by $\varphi(f_1), \ldots, \varphi(f_\ell)$, and its dual code C_ℓ.

Let F/K be an algebraic function field of one variable [Sti93], Q a place of degree one of F/K, v_Q the discrete valuation at Q, and $\mathscr{L}(\infty Q) = \bigcup_{i=0}^{\infty} \mathscr{L}(iQ)$. Then $-v_Q$ is a weight function on the ring $\mathscr{L}(\infty Q)$. Let $P_1, \ldots, P_n$ be pairwise distinct places of degree one, and $\varphi : \mathscr{L}(\infty Q) \to K^n$, $f \mapsto (f(P_1), \ldots, f(P_n))$. Then φ is an epimorphism of K-algebras, E_ℓ is a functional one-point algebraic geometry code, and C_ℓ is a residual one.

Let $g = \sharp\{m \in \mathbf{N}_0 \mid \text{there is no } f \in R \text{ such that } \rho(f) = m\}$. By elementary arguments we can show that E_ℓ is an $[n, \ell, d]$ code such that $d \ge n + 1 - \ell - g$ if $\rho(f_\ell) < n$ [HvLP98, Corollary 5.19], and the minimum distance of C_ℓ is at least $\ell + 1 - g$ [HvLP98, Theorem 5.24]. They correspond to the Goppa bound for the minimum distance of algebraic geometry codes.

2.2 Relation between an evaluation code and a one-point AG code

It is interesting what we can say about a ring with a weight function. The following is known.

Theorem 2.3 [Mat99b] *Let R be a K-algebra with a weight function ρ and $R \neq K$. Then there exist an algebraic function field F/K, its place Q of degree one, and a positive integer e such that F is the quotient field of R, $R \subseteq \mathscr{L}(\infty Q) = \bigcup_{i=0}^{\infty} \mathscr{L}(iQ)$, and $\rho = -e \times v_Q$. In other words, there exist a projective algebraic curve χ defined over K and a K-rational point $Q \in \chi$ such that R is the ring of K-rational functions regular at $\chi \setminus \{Q\}$ and ρ is a multiple of the pole order of rational functions at Q. In particular, R is finitely generated over K, and is an integral domain.*

Hereafter we call a K-algebra with a weight function a *weight domain*.

Evaluation codes and their duals are generalization of one-point AG codes. It is interesting whether we can obtain a good linear code as (the dual of) an evaluation code that is never obtained as a one-point AG code. Suppose that R is a weight domain with a weight function ρ. If R is integrally closed, then the evaluation code E_ℓ and its dual C_ℓ can be obtained as one-point AG codes. Thus to compare evaluation codes and ordinary AG codes, it is enough to compare evaluation codes (and its duals) on R with evaluation codes (and its duals) on the normalization of R. It is shown that we cannot obtain an evaluation code on R better than that on the normalization of R [Mat99a]. For precise statements, see [Mat99a].

3 Construction of weight domains

3.1 Construction of general weight domains

In this section, we review a class of defining equations which yields all weight domains. The results in this section were already shown in [Miu97, Miu98, Pel], and they were in part shown in the earlier paper [Miu94]. But our proofs are new and simpler than the original given in [Miu97, Miu98] and similar to the proofs in [Pel]. The second author proved his results [Miu97, Miu98] using the theory of algebraic function fields [Sti93], while we prove all the results in an elementary way. Note that the second author did not know the notion of weight domains and he did not state facts in his papers [Miu94, Miu97, Miu98] in the framework of the weight domain.

Let H be a subsemigroup of $\mathbf{N}_0$. We call $\{\rho(f) \mid 0 \neq f \in R\}$ the *associated semigroup* of a weight domain R with a weight function ρ. We shall consider a weight domain R with the associated semigroup H.

Lemma 3.1 *If $H = \{0\}$ then $R = K$.*

Proof. Let $x \in R$ and $\rho(x) = 0$. By the condition 4 in Definition 2.1, there exists $c \in K$ such that $\rho(x - c) = -\infty$, which implies $x = c$. ■

So we assume that $H \neq \{0\}$. $\mathbf{N}_0 \setminus H$ is finite iff the greatest common divisor of H is 1 [HvLP98, Corollary 5.12]. $\rho/\gcd(H)$ is also a weight function on R. So we may assume without loss of generality that $\mathbf{N}_0 \setminus H$ is finite by replacing ρ with $\rho/\gcd(H)$ if necessary. If $H = \mathbf{N}_0$ then R is the univariate polynomial ring over K [Mat99b]. So hereafter we also assume that $H \neq \mathbf{N}_0$.

Suppose that $A_t = \{a_1, \ldots, a_t\}$ is a generating set of H and $a_i \neq 0$ for $i = 1, \ldots, t$. We shall introduce a monomial order induced from A_t.

Definition 3.2 *For $(m_1, \ldots, m_t)$, $(n_1, \ldots, n_t) \in \mathbf{N}_0^t$, we define $(m_1, \ldots, m_t) \succ (n_1, \ldots, n_t)$ if*

$$a_1m_1 + \cdots + a_tm_t > a_1n_1 + \cdots + a_tn_t,$$

or

$$a_1m_1 + \cdots + a_tm_t = a_1n_1 + \cdots + a_tn_t,$$

and $m_1 = n_1$, $m_2 = n_2, \ldots, m_{i-1} = n_{i-1}$, $m_i < n_i$, for some $1 \leq i \leq t$.

Notice that the definition of $\succ$ depends on the order of elements in A_t.

Definition 3.3 [Miu94, Definition 6 and 8], [Miu97, Section 5.2], [Miu98, pp. 1408–1409] *We define $B(A_t) = \{(n_1, \ldots, n_t) \in \mathbf{N}_0^t \mid$ if $a_1n_1 + \cdots + a_tn_t = a_1m_1 + \cdots + a_tm_t$ for some $(m_1, \ldots, m_t) \in \mathbf{N}_0^t$ then $(n_1, \ldots, n_t) \preceq (m_1, \ldots, m_t)\}$, and $V(A_t)$ to be the set of minimal elements in $\mathbf{N}_0^t \setminus B(A_t)$ with respect to the partial order in $\mathbf{N}_0^t$ such that $(m_1, \ldots, m_t)$ is smaller than $(n_1, \ldots, n_t)$ if $m_i \leq n_i$ for $i = 1, \ldots, t$.*

Choose $x_i \in R$ such that $\rho(x_i) = a_i$. Let X_i be variable over K for $i = 1, \ldots, t$, and $I \subset K[X_1, \ldots, X_t]$ the kernel of the evaluation homomorphism $X_i \mapsto x_i$. We shall show that $R = K[x_1, \ldots, x_t]$ (Corollary 3.5), and characterize the form of the reduced Gröbner basis for I with respect to $\prec$ (Theorem 3.10). Then we shall show that if a set of polynomials is in such a form then it defines a weight domain conversely (Theorem 3.11). Basic facts in the Gröbner basis theory can be found in [AL94, CLO96]. We assume that the reader is familiar with Gröbner bases. For $N = (n_1, \ldots, n_t) \in \mathbf{N}_0^t$, we denote $X_1^{n_1} \cdots X_t^{n_t}$ (resp. $x_1^{n_1} \cdots x_t^{n_t}$) by X^N (resp. x^N).

Proposition 3.4 [Miu94, Lemma 10], [Miu97, Lemma 5.13], [Miu98, p. 1410] *$\{x^N \mid N \in B(A_t)\}$ forms a K-basis for R.*

Proof. By the definitions of $B(A_t)$ and the weight function, the elements in $\{x^N \mid N \in B(A_t)\}$ are linearly independent.

Let h be a nonzero element in R. There exists $N \in B(A_t)$ such that $\rho(x^N) = \rho(h)$, and $c_N \in K$ such that $\rho(h - c_Nx^N) < \rho(h)$. By repeating this argument, we can write h as

$$\sum_{N \in B(A_t)} c_Nx^N.$$

We have shown that h can be written as a linear combination of elements in $\{x^N \mid N \in B(A_t)\}$. ■

Corollary 3.5 [Miu94, Lemma 9], [Miu97, Lemma 5.3], [Miu98, p. 1406] $R = K[x_1, \ldots, x_t]$. ■

Definition 3.6 *The delta set of I, denoted by $\Delta(I)$, is $\{N \in \mathbf{N}_0^t \mid X^N$ is not the leading monomial of any nonzero polynomial in I with respect to $\prec\}$.*

Lemma 3.7 [Miu97, Section 5.4], [Miu98, p. 1417] $\Delta(I) = B(A_t)$.

Proof. We claim that $\Delta(I) \subseteq B(A_t)$. Suppose that there is $N \in \Delta(I) \setminus B(A_t)$. By Proposition 3.4, we can write x^N as

$$\sum_{\substack{M \in B(A_t) \\ \rho(x^M) \leq \rho(x^N)}} c_Mx^M.$$

Consider the polynomial
$$X^N - \sum_{\substack{M \in B(A_t) \\ \rho(x^M) \leq \rho(x^N)}} c_M X^M.$$

Then it belongs to I and by the definition of $B(A_t)$ its leading monomial is X^N, which is a contradiction.

Since $\{x^N \mid N \in \Delta(I)\}$ forms a K-basis for R [AL94, Proposition 2.1.6], we can see that $\Delta(I) = B(A_t)$ by Proposition 3.4. ■

Lemma 3.8 [Miu94, Lemma 7], [Miu97, Lemma 5.10], [Miu98, p. 1409] *$V(A_t)$ is finite.*

Proof. The assertion is a special case of Dickson's Lemma [AL94, Exercise 1.4.12]. ■

Definition 3.9 *For each $N \in V(A_t)$, we can write x^N as*
$$\sum_{M \in B(A_t)} c_M x^M,$$
in a unique way. We define the polynomial $F_N \in K[X_1, \ldots, X_t]$ to be
$$X^N - \sum_{M \in B(A_t)} c_M X^M.$$

Theorem 3.10 [Miu94, Lemma 14], [Miu97, Theorem 5.16], [Miu98, pp. 1410–1411] *$\{F_N \mid N \in V(A_t)\}$ is the reduced Gröbner basis for I with respect to $\prec$.*

Proof. $F_N \in I$ for each $N \in V(A_t)$, and $\{X^N \mid N \in V(A_t)\}$ is the set of minimal elements in the set of leading monomials of I. Thus by the definition of Gröbner basis, $\{F_N \mid N \in V(A_t)\}$ is a Gröbner basis. It is clear that $\{F_N \mid N \in V(A_t)\}$ is the reduced Gröbner basis for I. ■

We shall prove a converse to Theorem 3.10.

Theorem 3.11 [Miu94, Theorem 1], [Miu97, Theorem 5.17], [Miu98, p. 1411], [Pel, Theorem 5.11] *For $M = (m_1, \ldots, m_t) \in \mathbf{N}_0^t$, we define $\Psi(M) = a_1 m_1 + \cdots + a_t m_t$. For each $N \in V(A_t)$ choose a polynomial G_N in $K[X_1, \ldots, X_t]$ of the form*
$$X^N + c_M X^M + \sum_{L \in B(A_t),\, \Psi(L) < \Psi(N)} c_L X^L,$$
such that $\Psi(N) = \Psi(M)$, $M \in B(A_t)$, and $c_M \neq 0$. Let J be the ideal generated by $\{G_N \mid N \in V(A_t)\}$. If $\{G_N \mid N \in V(A_t)\}$ is a Gröbner basis (automatically becoming the reduced one) with respect to $\prec$, then $K[X_1, \ldots, X_t]/J$ is a weight domain with the weight function $\rho(X^L \bmod J) = \Psi(L)$ for $L \in B(A_t)$.

Proof. Notice that $V(A_t) + \mathbf{N}_0^t = \mathbf{N}_0^t \setminus B(A_t)$. Since $\{G_N \mid N \in V(A_t)\}$ is a Gröbner basis, $\Delta(J) = \mathbf{N}_0^t \setminus (V(A_t) + \mathbf{N}_0^t)$. Thus $\Delta(J) = B(A_t)$ and $\{X^L \bmod J \mid L \in B(A_t)\}$ forms a K-basis for $K[X_1, \ldots, X_t]/J$.

We shall check whether ρ is a weight function. The conditions 1–4 of weight functions (Definition 2.1) are satisfied by the discussion in the previous paragraph. We shall check the condition 5. Let E_1, E_2 be polynomials written as linear combinations of monomials in $\{X^N \mid N \in B(A_t)\}$. In order to calculate the weight of $E_1 E_2 \bmod J$, we have to write E_1E_2 as a linear combination of monomials in $\{X^N \mid N \in B(A_t)\}$, which can be done by Gröbner basis division. Let E_3 be the remainder on division of E_1E_2 by $\{G_N \mid N \in V(A_t)\}$. By the form of $\{G_N \mid N \in V(A_t)\}$, we can see that $\rho(E_1E_2 \bmod J) = \rho(E_3 \bmod J)$. ■

Remark 3.12 *In this survey a weight function has values in* $\mathbf{N}_0$. *Pellikaan and Geil* [Gei99] *extend the notion of weight functions to taking values in a general semigroup and genelarize Theorem* 3.11 *in* [Gei99, Theorem 1.7.1].

Proposition 3.13 [Miu97, Lemma 5.21], [Miu98, p. 1413] *We retain notations from Theorem* 3.11. $\rho(X^L \bmod J) = \Psi(L)$ *for all* $L \in \mathbf{N}_0^t$.

Proof. In order to calculate $\rho(X^L \bmod J)$, we have to write $X^L \bmod J$ as a linear combination of $\{X^{L'} \bmod J \mid L' \in B(A_t)\}$, which can be done by dividing X^L by $\{G_N \mid N \in V(A_t)\}$. Let L'' be the exponent of the leading monomial of the remainder on division of X^L by $\{G_N \mid N \in V(A_t)\}$. Then by definition $\rho(X^L \bmod J) = \Psi(L'')$. By the form of $\{G_N \mid N \in V(A_t)\}$, we can see that $\Psi(L) = \Psi(L'')$. ■

Remark 3.14 *When we construct a weight domain as in Theorem* 3.11*, we can easily find a K-basis for the weight domain with pairwise distinct weights as in the proof of Theorem* 3.11*. Such a basis is indispensable with code construction and decoding algorithms of AG codes. This fact is stated in a different way in* [SH95, Proposition 13].

Remark 3.15 *Saints and Heegard defined the notion of a projective algebraic curve in special position* [SH95, Definition 11]. *The projective closure of the affine algebraic curve defined in Theorem* 3.11 *is in special position if it is nonsingular and* $a_1 < \cdots < a_t$. *Conversely, if a projective algebraic curve* χ *is in special position with respect to a point Q, then the affine coordinate ring of the affine algebraic curve* $\chi \setminus \{Q\}$ *is a weight domain.*

For construction of weight domains and linear codes on them, we have to calculate $B(A_t)$ and $V(A_t)$. It is not obvious how to calculate $B(A_t)$ and $V(A_t)$. We shall clarify it.

Definition 3.16 *For* $i = 0, \ldots, a_1 - 1$, *we define* $b_i = \min\{x \in H \mid x \equiv i \pmod{a_1}\}$, *and* L_i *to be the minimum element* $N \in \mathbf{N}_0^t$ *with respect to* $\prec$ *such that* $\Psi(N) = b_i$, *where* Ψ *is as in Theorem* 3.11.

Notice that we can easily calculate $L_0, \ldots, L_{a_1-1}$ when we are given a sequence $a_1, \ldots, a_t$.

Lemma 3.17 *Let* $L_i = (\ell_1, \ldots, \ell_t)$. *Then* $\ell_1 = 0$.

Proof. Suppose that $\ell_1 > 0$. Then $b_i = \ell_1 a_1 + \ell_2 a_2 + \cdots + \ell_t a_t > \ell_2 a_2 + \cdots + \ell_t a_t \in H$, which contradicts to the definition of b_i. ■

Proposition 3.18 [Miu94, Lemma 5 and 7], [Miu97, Lemma 5.9 and 5.10], [Miu98, pp. 1408–1409] *Let*

$$e_i = (\overbrace{0, \ldots, 0}^{i-1}, 1, 0, \ldots, 0) \in \mathbf{N}_0^t,$$

for $i = 2, \ldots, t$. *Then*

$$\begin{aligned} B(A_t) &= \{L_i + (j, 0, \ldots, 0) \mid 0 \le i \le a_1 - 1,\ 0 \le j\}, \\ V(A_t) &\subseteq \{L_i + e_j \mid 0 \le i \le a_1 - 1,\ 2 \le j \le t\}. \end{aligned}$$

Proof. The second assertion follows from the first and the definition of $V(A_t)$. We shall prove the first.

Let $x \in H$, $i = x \bmod a_1$, and $j = (x - b_i)/a_1$. Then $x = b_i + ja_1$, and $\Psi(L_i + (j, 0, \ldots, 0)) = x$. Suppose that $\Psi(N) = x$ for some $N \in \mathbf{N}_0^t$. It is enough to show that $L_i + (j, 0, \ldots, 0) \preceq N$ to prove the first assertion by the definition of $B(A_t)$.

Let $N = (n_1, \ldots, n_t)$. If $n_1 < j$ then $L_i + (j, 0, \ldots, 0) \prec N$ by the definition of $\prec$. If $n_1 > j$ then $\Psi(0, n_2, \ldots, n_t) = x - n_1 a_1 < x - ja_1 = b_i$, which is a contradiction. So hereafter we assume that $j = n_1$.

Since $\prec$ is a monomial order, it is enough to show that $L_i \preceq (0, n_2, \ldots, n_t)$. Because $\Psi(0, n_2, \ldots, n_t) = b_i$, $L_i \preceq (0, n_2, \ldots, n_t)$ by the definition of L_i. ■

3.2 Construction of telescopic weight domains

It is difficult to check whether a given set of polynomials in Theorem 3.11 is a Gröbner basis by hand. We shall show that if H is telescopic then the set of polynomials in Theorem 3.11 automatically forms a Gröbner basis and we can write $B(A_t)$ and $V(A_t)$ in a more explicit way than Proposition 3.18. We call a weight domain telescopic if the associated semigroup is telescopic.

Definition 3.19 *A sequence $a_1, \ldots, a_t$ is said to be* telescopic *if a_i/d_i belongs to the semigroup generated by $a_1/d_{i-1}, \ldots, a_{i-1}/d_{i-1}$ for $i = 2, \ldots, t$, where d_i is the greatest common divisor of $a_1, \ldots, a_i$. A subsemigroup of $\mathbf{N}_0$ is said to be telescopic if it can be generated by a telescopic sequence.*

Lemma 3.20 *Let L_i be as in Definition* 3.16. *If $a_1, \ldots, a_t$ is telescopic, then $\{L_i \mid i = 0, \ldots, a_1 - 1\} = \{(0, n_2, \ldots, n_t) \mid 0 \le n_i < d_{i-1}/d_i$ for $i = 2, \ldots, t\}$.*

Proof. Suppose that $L_i = (0, \ell_2, \ldots, \ell_t)$, and $\ell_j \ge d_{j-1}/d_j$ for some $j \ge 2$. By the definition of telescopic sequences, $(d_{j-1}/d_j)a_j$ belongs to the semigroup generated by $a_1, \ldots, a_{j-1}$. Let $\alpha_1 a_1 + \cdots + \alpha_{j-1} a_{j-1} = (d_{j-1}/d_j)a_j$, and $L'_i = (\ell_1 + \alpha_1, \ldots, \ell_{j-1} + \alpha_{j-1}, \ell_j - (d_{j-1}/d_j), \ell_{j+1}, \ldots, \ell_t)$. Then $\Psi(L_i) = \Psi(L'_i)$ and $L'_i \prec L_i$, which contradicts to the definition of L_i. We have shown that $\{L_i \mid i = 0, \ldots, a_1 - 1\} \subseteq \{(0, n_2, \ldots, n_t) \mid 0 \le n_i < d_{i-1}/d_i$ for $i = 2, \ldots, t\}$.

Is is easy to see that both sets have a_1 elements. So the assertion is proved. ■

Corollary 3.21 [Miu94, Theorem 1 (VI)], [Miu97, Theorem 5.43], [Miu98, p. 1419] *Suppose that the sequence $a_1, \ldots, a_t$ is telescopic. Then*

$$\begin{aligned} B(A_t) &= \{(n_1, \ldots, n_t) \in \mathbf{N}_0^t \mid 0 \le n_i < d_{i-1}/d_i \text{ for } i = 2, \ldots, t\}, \\ V(A_t) &= \{(\overbrace{0, \ldots, 0}^{i-1}, d_{i-1}/d_i, 0, \ldots, 0) \mid i = 2, \ldots, t\}. \end{aligned}$$

Proof. The assertions follow directly from the previous lemma, Proposition 3.18, and the definition of $\prec$ and $V(A_t)$. ■

Remark 3.22 *A similar fact to Corollary* 3.21 *is shown in* [KP95, Lemma 6.4] *and* [HvLP98, Lemma 5.34].

Theorem 3.23 [Miu94, p. 462, Remark], [Miu97, Corollary 5.36], [Miu98, p. 1418] *Suppose that $a_1, \ldots, a_t$ is telescopic. Then the set of polynomials $\{G_N \mid N \in V(A_t)\}$ forms a Gröbner basis.*

Proof. The assertion follows directly from Theorem 3 and Proposition 4 in [CLO96, Section 2.9]. ■

Remark 3.24 *A special case of the previous theorem is in* [HvLP98, Example 5.36], [Pel, Proposition 5.12].

Remark 3.25 *Further applications of telescopic semigroups in coding theory can be found in* [HvLP98, KP95]. *Research articles on telescopic semigroups are listed in* [KP95, Remark 6.7].

Remark 3.26 *It is desirable to choose generators $a_1, \dots, a_t$ as few as possible. A generating set of H is said to be* minimal *if H is not generated by its proper subset. We can prove that a minimal generating set is unique, each generating set contains the minimal one, and if H is telescopic then we can make the minimal generating set a telescopic sequence. A proof can be found in* [Miu97, Miu98].

3.3 Construction of plane weight domains

If the associated semigroup is generated by two numbers, then the weight domain can be obtained as the affine coordinate ring of a plane affine algebraic curve. We call such a weight domain plane. In this subsection we write down the defining equation of a plane weight domain explicitly.

We retain notations from Section 3.1 unless otherwise specified. Let $a = a_1$, $b = a_2$, $X = X_1$, and $Y = X_2$. Since we assume that $\mathbf{N}_0 \setminus H$ is finite and not empty, a and b are relatively prime [HvLP98, Corollary 5.12] and greater than 1. Note that in this case a, b is a telescopic sequence and a plane weight domain is a special case of a telescopic weight domain.

As a special case of Corollary 3.21 we have

Corollary 3.27 [Miu97, Section 7.2]

$$\begin{aligned} B(A_t) &= \{(i,j) \in \mathbf{N}_0^2 \mid 0 \le i,\ 0 \le j < a\}, \\ V(A_t) &= \{(0,a)\}. \end{aligned}$$

F_N in Theorem 3.10 *and G_N in Theorem* 3.11 *is of form*

$$Y^a + c_{b,0}X^b + \sum_{ia+bj<ab} c_{i,j}X^iY^j, \tag{1}$$

where $c_{b,0} \neq 0$ and $c_{i,j} \in K$. ■

We shall clarify which algebraic curve can have a plane model of the form (1).

Proposition 3.28 [Miu97, Theorem 5.17 (9)], [Miu98, p. 1412] *Let χ be a nonrational nonsingular projective algebraic curve over K. If there is a K-rational point $Q \in \chi$, then χ can have a plane model of the form* (1).

Proof. Let F be the field of K-rational functions on χ, v_Q the discrete valuation at Q, and $x,y \in F \setminus K$ functions such that they are regular at $\chi \setminus \{Q\}$ and $v_Q(x)$ and $v_Q(y)$ are relatively prime. From the definition of x,y, the pole divisor of x (resp. y) is $-v_Q(x)Q$ (resp. $-v_Q(y)Q$).

$[F : K(x)] = -v_Q(x)$ and $[F : K(y)] = -v_Q(y)$ [Sti93, Theorem I.4.11], and $[F : K(x,y)]$ divides both $[F : K(x)]$ and $[F : K(y)]$. Thus $[F : K(x,y)] = 1$.

$K[x,y]$ is a weight domain with the weight function $-v_Q$. Thus $K[x,y]$ is the affine coordinate ring of an affine algebraic curve defined by a polynomial of the form (1), where we set $a = -v_Q(x)$ and $b = -v_Q(y)$. ■

Remark 3.29 *The second author observed that we can easily construct algebraic geometry codes on affine algebraic curves defined by polynomials of form* (1) *in* [Miu92].

Remark 3.30 *An overlapping but different construction of weight domains is in* [HvLP98, Proposition 3.17], [Pel, Proposition 4.6].

References

[AL94] William W. Adams and Phillippe Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.

[CLO96] David Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, 2nd ed., Springer-Verlag, Berlin, 1996.

[Gei99] Olav Geil, *Codes based on an $\mathbb{F}_q$-algebra*, Ph.D. thesis, Aalborg Univ., Denmark, December 1999.

[HvLP97] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan, *Order functions and evaluation codes*, Proc. AAECC-12, Lecture Notes in Computer Science, vol. 1255, Springer-Verlag, 1997, pp. 138–150.

[HvLP98] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan, *Algebraic geometry codes*, Handbook of Coding Theory (Vera Pless and William Cary Huffman, eds.), Elsevier, 1998, pp. 871–961.

[KP95] Christoph Kirfel and Ruud Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 1720–1732.

[Mat99a] Ryutaroh Matsumoto, *Linear codes on nonsingular curves are better than those on singular curves*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (ISSN 0916-8508) **E82-A** (1999), no. 4, 665–670.

[Mat99b] Ryutaroh Matsumoto, *Miura's generalization of one-point AG codes is equivalent to Høholdt, van Lint and Pellikaan's generalization*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (ISSN 0916-8508) **E82-A** (1999), no. 10, 2007–2010.

[Miu92] Shinji Miura, *Algebraic geometric codes on certain plane curves*, Transactions of IEICE (ISSN 0913-5707) **J75-A** (1992), no. 11, 1735–1745 (Japanese).

[Miu94] Shinji Miura, *Constructive theory of algebraic curves*, Proceedings of the 17th Symposium on Information Theory and Its Applications (Hiroshima, Japan), December 1994, pp. 461–464 (Japanese).

[Miu97] Shinji Miura, Ph.D. thesis, Univ. Tokyo, May 1997 (Japanese).

[Miu98] Shinji Miura, *Linear codes on affine algebraic curves*, Transactions of IEICE (ISSN 0913-5707) **J81-A** (1998), no. 10, 1398–1421 (Japanese).

[Pel] Ruud Pellikaan, *On the existence of order functions*, to appear in Journal of Statistical Planning and Inference, available from `http://www.win.tue.nl/math/dw/personalpages/ruudp/`.

[SH95] Keith Saints and Chris Heegard, *Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Gröbner bases*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 1733–1751.

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.