PAPER

Linear Codes on Nonsingular Curves are Better than Those on Singular Curves*

Ryutaroh MATSUMOTO[†], *Member*

SUMMARY Recently, Miura introduced a construction method of one-point algebraic geometry codes on singular curves, which is regarded as a generalization of one on nonsingular curves, and enables us to construct codes on wider class of algebraic curves. However, it is still not clear whether there really exist singular curves on which we can construct good codes that are never obtained from nonsingular curves. In this paper, we show that for fixed designed minimum distance in a wide range, the dimension of codes on a singular curve is smaller than or equal to that of the codes on its normalization, and the number of check symbols of the former codes is larger than that of the latter codes. This implies the optimality of nonsingular curves for code construction.

key words: *algebraic geometry codes, singular curve, normalization*

1. Introduction

We needed nonsingular algebraic curves with Goppa's construction of linear codes on algebraic curves. Recently Miura generalized Goppa's construction to singular curves [7]. His generalization enlarged the class of algebraic curves available for code construction. However Miura has not clarified whether there are singular curves on which we can construct better codes than on nonsingular curves. It is well-known that performance of codes on algebraic curves with many rational points is better than those with fewer rational points and the same genus. Since there is an example, see Example 4.1, in which we can increase the number of rational points by singularizing algebraic curve, there might be singular curves that give good codes.

For an affine algebraic curve χ, we call χ' the normalization of χ if the affine coordinate ring of χ' is isomorphic to the integral closure of the coordinate ring of χ [2, Exercise 3.17 in Chap. 1]. To determine whether there are singular curves giving good codes which cannot be constructed from nonsingular curves, it is enough to compare codes on a singular curve and its normalization. In this paper, we show that the dimension of codes on a singular curve is smaller than or equal to that of the codes on its normalization and the number of check symbol of the former is larger than the latter in a wide range of designed minimum distance. This implies nonsingular curves are optimal for code construction in a wide range of designed minimum distance.

In Sect. 2, we review mathematical facts used in the proofs of this paper. In Sect. 3, we review Miura's construction of linear codes on singular curves and find the condition under which the number of check symbols is completely determined by the gap number of curves and the designed minimum distance. In Sect. 4, we show that the increase of rational points is not greater than that of check symbols. In Sect. 5, the concluding remarks are given.

2. Notations and Preliminaries

In this section we review mathematical facts used in this paper. Let K be an arbitrary perfect field. An extension field F of a field K is said to be an *algebraic function field* over K, if the following two conditions are met:

1. There exists an element $x \in F$ which is transcendental over K so that F is a finite extension of $K(x)$.
2. K is algebraically closed in F.

A *discrete valuation* v of the function field F/K is a function $v : F \to \mathbf{Z} \cup \{\infty\}$ satisfying

1. $v(a) = \infty$ iff $a = 0$.
2. $v(ab) = v(a) + v(b)$, for all $a, b \in F \setminus \{0\}$.
3. There exists $a \in F$ such that $v(a) = 1$.
4. $v(a + b) \geq \min\{v(a), v(b)\}$, for all $a, b \in F$.
5. $v(a) = 0$, for all $a \in K \setminus \{0\}$.

Proposition 2.1 (Strict Triangle Inequality [9]): If $v(a) \neq v(b)$ then $v(a + b) = \min\{v(a), v(b)\}$. □

For each discrete valuation v_P of F/K there is an associated *discrete valuation ring* $O_P = \{a \in F \mid v_P(a) \geq 0\}$. A discrete valuation ring O_P is a local ring and its unique maximal ideal P is called a *place* in F/K and we denote by $\mathbf{P}_F$ the set of place in F/K.

We can find an element in F with specified values of discrete valuations by the following proposition.

Proposition 2.2 (Strong Approximation Theorem [9]): Let S be a proper subset of $\mathbf{P}_F$ and $P_1, \ldots, P_r \in S$. Suppose there are given $x_1, \ldots, x_r \in F$ and integers

Manuscript received June 5, 1998.

[†]The author is in the Sakaniwa Lab., the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology, Tokyo, 152–8552 Japan.

*The results in this paper were partially presented at IEICE Information Theory Workshop [4].

$n_1, \ldots, n_r$. Then there exists an element $x \in F$ such that

$$v_{P_i}(x - x_i) = n_i \ \ (i = 1, \ldots, r), \ \text{and}$$
$$v_P(x) \geq 0, \ \forall P \in S \setminus \{P_1, \ldots, P_r\}.$$

□

A *divisor* D in F/K is a formal sum of places $\sum n_P P$ where n_P is an integer and $n_P = 0$ except for finitely many places P in F/K. We define $v_P(D) := n_P$. Support of divisor D, $\operatorname{supp} D$, is the set of places P such that $n_P \neq 0$. For a divisor D,

$$L(D) := \{f \in F \mid \forall P, \ v_P(f) \geq -v_P(D)\} \cup \{0\}.$$

$L(D)$ is a finite-dimensional vector space over K.

For subring R in F, $x \in F$ is said to be *integral* over R iff there exists elements $a_0, \ldots, a_{m-1} \in R$ such that $x^m + a_{m-1}x^{m-1} + \cdots + a_0 = 0$. *Integral closure* of R in F is the overring $\{x \in F \mid x \text{ is integral over } R\}$. If integral closure of R is R itself then R is said to be *integrally closed.*

A subring R in F is said to be a *holomorphy ring* if there exists a nonempty proper subset S of $\mathbf{P}_F$ such that $R = \bigcap_{P \in S} O_P$. We denote $\bigcap_{P \in S} O_P$ by O_S. A holomorphy ring is integrally closed in F and its quotient field is F. For subring R in F with its quotient field F, integral closure of R is a holomorphy ring.

Proposition 2.3: For a finite set of places S, a holomorphy ring $O_S = \bigcap_{P \in S} O_P$ and a nonzero ideal $I \subseteq O_S$, we define $D := \sum_{P \in S} \min\{v_P(x) \mid x \in I\}P$. Then for $x \in O_S$,

$$x \in I \setminus \{0\} \Leftrightarrow \forall P \in \operatorname{supp} D, \ v_P(x) \geq v_P(D).$$

Proof: Since O_S is a principal ideal domain by [9, Proposition III.2.10], $I = tO_S$ for some $t \in O_S$. Then

$$v_P(t) = v_P(D), \forall P \in S,$$

and the assertion follows. □

3. Codes on Singular Curves and Their Designed Minimum Distance

In this section we review Miura's construction of linear codes on singular curves and give the condition when the number of check symbols of a code is completely determined by its designed minimum distance and the gap number of the curve.

3.1 Miura's Generalization

In this subsection we review [7]. $\mathbf{F}_q$ denotes the finite field with q elements and let $F/\mathbf{F}_q$ be an algebraic function field. For a place Q of degree one,

$$L(\infty Q) := \bigcup_{i=1}^{\infty} L(iQ) = \bigcap_{P \in \mathbf{P}_F \setminus \{Q\}} O_P.$$

We fix a place Q of degree one in $F/\mathbf{F}_q$. Let R be a subring of $L(\infty Q)$. R is finitely generated over $\mathbf{F}_q$, in other words there exists $\{y_1, \ldots, y_t\} \subset L(\infty Q)$ such that $R = \mathbf{F}_q[y_1, \ldots, y_t]$. Let $\mathbf{F}_q[Y_1, \ldots, Y_t]$ be a polynomial ring in t variables over $\mathbf{F}_q$ and consider the following evaluation map:

$$\mathbf{F}_q[Y_1, \ldots, Y_t] \longrightarrow R$$
$$f(Y_1, \ldots, Y_t) \longmapsto f(y_1, \ldots, y_t).$$

Then the kernel of the map defines an affine algebraic curve in t-dimensional affine space and we will identify R with the curve. A curve having $L(\infty Q)$ as its affine coordinate ring is the normalization of a curve having R as its affine coordinate ring.

For a commutative ring A containing $\mathbf{F}_q$, $\mathrm{MSpec}(A)$ is the set of maximal ideals in A. For $M \in \mathrm{MSpec}(A)$, we define the degree of M as $[A/M : \mathbf{F}_q]$. Let $N(A)$ denote the number of maximal ideals of degree one in A. There is a 1-1-correspondence between maximal ideals in R of degree one and $\mathbf{F}_q$-rational points in R. To see this, let M be a maximal ideal of degree one in R and we set $a_i := y_i \bmod M \in \mathbf{F}_q$ for $i = 1, \ldots, t$. Then the ideal $(Y_1 - a_1, \ldots, Y_t - a_t)$ contains the defining ideal I of the curve R and $(a_1, \ldots, a_t)$ is the corresponding $\mathbf{F}_q$-rational point of M.

Let $\{M_1, \ldots, M_{N(R)}\}$ be the set of all maximal ideals of degree one in R. We define a map ϕ from R to $\mathbf{F}_q^{N(R)}$ as

$$R \longrightarrow \mathbf{F}_q^{N(R)}$$
$$x \longmapsto (x \bmod M_1, \ldots, x \bmod M_{N(R)})$$

For a set $\cdot$, $\langle \cdot \rangle$ denotes the vector space spanned by $\cdot$. $\{f_1 = 1, f_2, \ldots, \}$ is a basis of R as $\mathbf{F}_q$-vector space such that $v_Q(f_{i-1}) > v_Q(f_i)$ and

$$\{g_1 = 1, \ldots, g_{N(R)}\}$$
$$:= \{f_i \mid \phi(f_i) \notin \langle \phi(f_1), \ldots, \phi(f_{i-1}) \rangle\},$$

where $v_Q(g_{i-1}) > v_Q(g_i)$. B_i denotes $\langle \phi(g_1), \ldots, \phi(g_i) \rangle$ and we set $B_0 := \{0\}$.

Definition 3.1: For $1 \leq s \leq N(R)$, we define $M(s) := \{(i, j) \mid \phi(g_i g_j) \in B_s \setminus B_{s-1}$ and for $1 \leq u \leq i$, $1 \leq v \leq j$, $(u, v) \neq (i, j)$, $\phi(g_u g_v) \in B_{s-1}\}$ and $m_s := \#M(s)$.

For $\mathbf{F}_q$-vector space W, $W^{\perp}$ denotes the dual space of W.

Proposition 3.2: [6, Theorem 3.4 and 3.5] For a linear code

$$C(R, d) := \langle \{\phi(g_s) \mid m_s \leq d - 1\} \rangle^{\perp},$$

we can correct up to $\lfloor (d-1)/2 \rfloor$ errors by the Feng-Rao decoding algorithm. □

By the proposition above, m_s is larger, the number of check symbols of $C(R, d)$ is smaller for a given designed minimum distance. There is a lower bound for m_s.

Definition 3.3: The gap number $G(R)$ of R is the number of non-positive integers not belonging to $v_Q(R)$.

Proposition 3.4: $s \geq m_s \geq s - G(R)$. □

If R is strictly contained in $L(\infty Q)$, $G(R) > G(L(\infty Q))$, the number of check symbols of $C(L(\infty Q), d)$ seems to be smaller than that of $C(R, d)$, but it is not clear. In the next subsection we show that it is the case in a wide range of designed minimum distance.

3.2 When is the Number of Check Symbols Determined by $G(R)$?

Lemma 3.5: The restriction $\phi|\langle g_1, \ldots, g_{N(R)-G(R)}\rangle$ is injective.

Proof: This is the immediate consequence of [7, p.1402, Lemma]. □

Lemma 3.6: [7, p.1402, Lemma] For $G(R)+1 \leq s \leq N(R) - G(R)$, $-v_Q(g_s) = s - 1 + G(R)$. This implies that for $2G(R) \leq i \leq N(R)-1$, there exists $G(R)+1 \leq s \leq N(R) - G(R)$ such that $-i = v_Q(g_s)$. □

Lemma 3.7: If $s \leq N(R) - G(R)$ and $N(R) \geq 4G(R) + 1$, then $(i, j) \in M(s)$ if and only if $v_Q(g_s) = v_Q(g_i g_j)$.

Proof: It is clear that if $v_Q(g_s) = v_Q(g_i g_j)$ then $(i, j) \in M(s)$.

We will prove that if $v_Q(g_s) \neq v_Q(g_i g_j)$ then $(i, j) \notin M(s)$. If $v_Q(g_s) < v_Q(g_i g_j)$ then $\phi(g_i g_j) \in B_{s-1}$ by Lemma 3.5 and $(i, j) \notin M(s)$.

From here we assume that $v_Q(g_s) > v_Q(g_i g_j)$

Case $v_Q(g_i g_j) > N(R)$**:** In this case,

$$g_i g_j \in \langle g_1, \ldots, g_{n-G(R)}\rangle \setminus \langle g_1, \ldots, g_s\rangle,$$

and $\phi(g_i g_j) \in B_{n-G(R)} \setminus B_s$ by Lemma 3.5. Thus $(i, j) \notin M(s)$.

Case $-N(R) \geq v_Q(g_i g_j)$**:** We can assume without loss of generality $v_Q(g_i) \leq v_Q(g_j)$.

Subcase $-N(R) + 1 - v_Q(g_j) \leq -2G(R)$**:** By Lemma 3.6 there exists $u < i$ such that $v_Q(g_u) = -N(R) + 1 - v_Q(g_j)$. Since $v_Q(g_u g_j) = -N(R) + 1 \leq v_Q(g_s)$ and $g_u g_j \notin \langle g_1, \ldots, g_{s-1}\rangle$, by Lemma 3.5 $\phi(g_u g_j) \notin B_{s-1}$, which implies $(i, j) \notin M(s)$.

Subcase $-N(R) + 1 - v_Q(g_j) > -2G(R)$**:** By assumption

$$\begin{aligned} -2G(R) &\geq -N(R) + 2G(R) + 1 \\ &> v_Q(g_j) \\ &\geq v_Q(g_i). \end{aligned}$$

By Lemma 3.6 there exists $1 \leq v < j$ such that $v_Q(g_v) = -2G(R)$, and $1 \leq u < i$ such that $v_Q(g_i) = -N(R) + 1 + 2G(R)$. Since $v_Q(g_u g_v) = -N(R) + 1 \leq v_Q(g_s)$, by Lemma 3.5 $\phi(g_u g_v) \notin B_{s-1}$ and $(i, j) \notin M(s)$. □

Lemma 3.8: We assume $4G(R) + 1 \leq N(R)$.

1. For $3G(R) \leq s \leq N(R) - G(R)$, $m_s = s - G(R)$.
2. For $s < 3G(R)$, $m_s \leq 2G(R)$.

Proof: This proof is based on [3, Theorem 3.8]. We define $T = \{-v_Q(g_i) \mid 1 \leq i \leq N(R) - G(R)\}$. For $l \in T$,

$$\begin{aligned} A(l) &:= \{(i, j) \mid i + j = l\}, \\ B(l) &:= \{(i, j) \in A(l) \mid i \notin T\}, \\ C(l) &:= \{(i, j) \in A(l) \mid j \notin T\}, \\ D(l) &:= B(l) \cap C(l), \end{aligned}$$

where i, j stand for nonnegative integers. We set $t = -v_Q(g_s)$. By the previous lemma,

$$m_s = \#A(t) - \#B(t) - \#C(t) + \#D(t).$$

If $s \geq G(R)+1$, $t = s+G(R)-1$ and $\#B(t) = \#C(t) = G(R)$ by [7, p.1402, Lemma]. Since $\#A(t) = t + 1 = s + G(R)$,

$$m_s = s - G(R) + \#D(t).$$

$2G(R) - 1$ is an upper bound for integer i such that $-i \notin v_Q(R)$. Hence for given t, candidates of elements in $D(t)$ are

$$\begin{gathered} (2G(R) - 1, t + 1 - 2G(R)), \\ (2G(R) - 2, t + 2 - 2G(R)), \\ \vdots \\ (t + 1 - 2G(R), 2G(R) - 1). \end{gathered}$$

This implies

$$\begin{aligned} &\#D(t) \leq 4G(R) - 1 - t \text{ if } t < 4G(R) - 1, \\ &\#D(t) = 0 \text{ if } t \geq 4G(R) - 1. \end{aligned}$$

This proves the statement. □

By the above observation, we find that the number of check symbols of $C(R, d)$ is completely determined by $G(R)$ in a certain range of d.

Theorem 3.9: If[†] $4G(R) + 1 \leq N(R)$, for $2G(R) + 1 \leq d \leq N(R)-2G(R)+1$ the number of check symbols in $C(R, d)$ is $d + G(R) - 1$.

Proof: By the previous lemma,

$$\{s \mid m_s \leq d - 1\} = \{1, 2, \ldots, d + G(R) - 1\}.$$

□

[†] Pellikaan and Torres showed that the assumption $2G(R) + 1 \leq d$ in Theorem 3.9 can be weaken [8].

4. The Number of $\mathbf{F}_q$-Rational Points in a Singular Curve and Its Normalization

Let R be an affine coordinate ring of some affine algebraic curve defined over $\mathbf{F}_q$ and assume that R is properly contained in $L(\infty Q)$ for some place of degree one in its function field $F/\mathbf{F}_q$. Then R is not a holomorphy ring of $F/\mathbf{F}_q$ and not integrally closed by [9, Cor. III.2.8]. Since an affine algebraic curve is nonsingular if and only if its affine coordinate ring is integrally closed, the affine algebraic curve having R as its coordinate ring is a singular curve.

$L(\infty Q)$ is the coordinate ring of the normalization of R by definition. $G(L(\infty Q))$ equals to the genus of $F/\mathbf{F}_q$ and strictly less than $G(R)$. Thus the number of check symbols of $C(L(\infty Q), d)$ is strictly less than that of $C(R, d)$ in a wide range of d. But $N(L(\infty Q))$ might be much less than $N(R)$ and it is not obvious whether $C(L(\infty Q), d)$ is better than $C(R, d)$. In this section we show that $N(R) - N(L(\infty Q)) \leq G(R) - G(L(\infty Q))$. Before giving proof, we present an example that $N(R)$ is greater than $N(L(\infty Q))$.

Example 4.1: Consider $F/\mathbf{F}_q = \mathbf{F}_{53}(x, y)/\mathbf{F}_{53}$ with $y^2 = x^3 + x$. It is an elliptic function field. If Q is the common pole of x and y then $L(\infty Q) = \mathbf{F}_{53}[x, y]$. It can be verified that $L(\infty Q)$ has 67 maximal ideals of degree one by counting solutions of $Y^2 - (X^3 + X) = 0 \pmod{53}$. Thus it has 68 rational points and it attains Serre upper bound [9, Th. V.3.1] for the number of rational points of a nonsingular curve. Let $z = x^2 + 5x + 25$ and consider $R = \mathbf{F}_{53}[y, z]$. The quotient field of R is F. Let J be an ideal in $\mathbf{F}_{53}[X, Y, Z]$ generated by $\{Y^2 - X^3 - X, Z - X^2 - 5X - 25\}$ and $I := J \cap \mathbf{F}_{53}[Y, Z]$. Then R is isomorphic to $\mathbf{F}_{53}[Y, Z]/I$ [1, Prop. 15.30]. I is generated by $27 + 33Y^2 + 52Y^4 + 52Z + 38Y^2Z + 33Z^2 + Z^3$. It can be verified that R has 69 maximal ideals of degree one by counting solutions of $27 + 33Y^2 + 52Y^4 + 52Z + 38Y^2Z + 33Z^2 + Z^3 = 0 \pmod{53}$. The number of rational points exceeds Serre bound. Since $v_Q(y) = -3$ and $v_Q(z) = -4$, $G(R) = 3$ and that is the maximal possible number of $\mathbf{F}_{53}$-rational points by the theorem proved later.

For $M \in \mathrm{MSpec}(R)$, we define its local ring O_M by the localization of R with respect to M, in other words $O_M = \{f/g \mid f \in R,\ g \in R \setminus M\}$. O'_M is its integral closure in F. We call M nonsingular if and only if $O_M = O'_M$. For a maximal ideal M of degree one, this definition is consistent with ordinary definition of singularity [2] of an $\mathbf{F}_q$-rational point.

Lemma 4.2:

$$R = \bigcap_{M \in \mathrm{MSpec}(R)} O_M,$$

$$L(\infty Q) = \bigcap_{M \in \mathrm{MSpec}(R)} O'_M$$

Proof: $\bigcap_{M \in \mathrm{MSpec}(R)} O_M = \{f/g \mid f \in R, g \in R \setminus \bigcup_{M \in \mathrm{MSpec}(R)} M\}$. For $x \in R \setminus \bigcup_{M \in \mathrm{MSpec}(R)} M$, the ideal (x) is R itself and $1 \in (x)$. Thus x is a unit of R. We have proved $R = \bigcap_{M \in \mathrm{MSpec}(R)} O_M$.

Since O'_M is a holomorphy ring and not contained in the discrete valuation ring O_Q, $L(\infty Q) \subset O'_M$ and the inclusion $L(\infty Q) \subseteq \bigcap_{M \in \mathrm{MSpec}(R)} O'_M$ is obvious.

For $M \in \mathrm{MSpec}(R)$ and $S := \{P \in \mathbf{P}_F \mid O_P \supset O_M\}$, by [9, Th. III.2.6]

$$O'_M = \bigcap_{P \in S} O_P.$$

Assume there is an element $x \in \bigcap_{M \in \mathrm{MSpec}(R)} O'_M \setminus L(\infty Q)$. Then there exists a place $P \in \mathbf{P}_F \setminus \{Q\}$ such that for all $M \in \mathrm{MSpec}(R)$, O_M is not contained in O_P. This implies R is not contained in O_P, which contradicts that R is a subring of $L(\infty Q)$. □

Definition 4.3: The conductor c_M of ring extension O'_M/O_M is

$$\{f \in O_M \mid \forall g \in O'_M,\ fg \in O_M\}.$$

In other words, c_M is the largest ideal in O_M which is also an ideal in O'_M.

Since a conductor c_M is a ideal in a holomorphy ring, by Proposition 2.3 we can identify c_M with a divisor and $\dim O'_M/c_M = \deg c_M < \infty$ by [1, Exercise 11.13 a], where $\dim O'_M/c_M$ is the dimension of $\mathbf{F}_q$-vector space O'_M/c_M. Thus $\dim O'_M/O_M < \infty$ by $c_M \subset O_M$, where O'_M/O_M is not a ring extension but a factor space.

Definition 4.4: For $M \in \mathrm{MSpec}(R)$,

$$\delta_M := \dim O'_M/O_M.$$

Lemma 4.5:

$$\dim L(\infty Q)/R = \sum_{M \in \mathrm{MSpec}(R)} \delta_M.$$

Proof: We explicitly construct an $\mathbf{F}_q$-basis of O'_M/O_M whose representatives belong to $L(\infty Q)$ and are linearly independent modulo R. Let $\{f_1 + O_M, \ldots, f_s + O_M\}$ be a basis of O'_M/O_M. By the strong approximation theorem we can find a function $g_{M,i} \in F$ for $i = 1, \ldots, s$ such that

$$\begin{aligned} &v_P(g_{M,i} - f_i) = v_P(c_M), \quad \forall P \in \operatorname{supp} c_M, \\ &v_P(g_{M,i}) = v_P(c_N), \quad \forall N \in \mathrm{MSpec}(R) \setminus \{M\}, \\ &\qquad\qquad O'_N \neq O_N, \\ &\qquad\qquad \forall P \in \operatorname{supp} c_N, \\ &v_P(g_{M,i}) \geq 0 \quad \forall P \in \mathbf{P}_F \setminus \{Q\}. \end{aligned}$$

By the first condition and the strict triangle inequality of discrete valuation, $v_P(g_{M,i}) \geq \min\{v_P(f_i), v_P(c_M)\}$ for $P \in \operatorname{supp} c_M$ and $i = 1, \ldots, s$. Thus $g_{M,i} \in O'_M$. Because $g_{M,i} = f_i \pmod{O_M}$, $\{g_{M,1} + O_M, \ldots, g_{M,s} +$

$O_M\}$ is a basis for O'_M/O_M. By the third condition $g_{M,i}$'s belong to $L(\infty Q)$. We construct $g_{N,i}$ for other singular points N. Finally we show $g_{M,i}$'s are linearly independent modulo R. Assume that

$$\sum_{i=1}^{s} a_i g_{M,i} + \sum_{\substack{i \\ N\in \mathrm{MSpec}(R)\setminus\{M\}, O'_N \neq O_N}} b_{N,i} g_{N,i} \in R,$$

where a_i, $b_{N,i}$'s belong to $\mathbf{F}_q$. The second summation is contained in $c_M \subset O_M$ and the first summation belongs to O_M. Since $\{g_{M,1}+O_M, \ldots, g_{M,s}+O_M\}$ is a basis of O'_M/O_M, this implies all a_i's are 0. Similar argument for other $N \neq M$ shows $b_{N,i}$'s are 0. We have proved $\dim R'/R \geq \sum_M \delta_M$. The converse inequality is obvious. □

Lemma 4.6:

$$\dim L(\infty Q)/R = G(R) - G(L(\infty Q)).$$

Proof: For each $j \in -v_Q(R\setminus\{0\})$, there is $\beta_j \in R$ such that $(\beta_j)_\infty = jP$. $\{\beta_j\}_{j\in -v_Q(R\setminus\{0\})}$ forms a basis of R as a $\mathbf{F}_q$-vector space. Let S be the set of nonnegative integer i such that $-i \in v_Q(L(\infty Q)) \setminus v_Q(R)$. Then for each $i \in S$, there exists $\alpha_i \in F$ such that $(\alpha_i)_\infty = iP$. $\{\alpha_i\}_{i\in S} \cup \{\beta_j\}_{j\in -v_Q(R\setminus\{0\})}$ forms a basis of $L(\infty Q)$ as a $\mathbf{F}_q$-vector space. This proves the lemma. □

We define a map ψ from $\mathrm{MSpec}(L(\infty Q))$ to $\mathrm{MSpec}(R)$ as

$$\begin{aligned} &\mathrm{MSpec}(L(\infty Q)) \longrightarrow \mathrm{MSpec}(R) \\ &M \longmapsto M \cap R \end{aligned}$$

We count the number of a maximal ideal $M \in \mathrm{MSpec}(R)$ of degree one such that for all $N \in \psi^{-1}M$, $\deg N > 1$. This ideal M corresponds to the $\mathbf{F}_q$-rational point in R which becomes not $\mathbf{F}_q$-rational by normalization.

Lemma 4.7: For $M \in \mathrm{MSpec}(R)$ of degree one, $\forall N \in \psi^{-1}M$, $\deg N > 1$ only if $\delta_M > 0$.

Proof: If $O_M = O'_M$, O_M is a holomorphy ring with a unique maximal ideal, thus is a discrete valuation ring in $F/\mathbf{F}_q$. Let P be its place. Then $\psi^{-1}M = \{P \cap L(\infty Q)\}$ and P is a unique maximal ideal of O'_M. $R/M \simeq O_M/P$ by the property of localization, where $\simeq$ denotes field-isomorphism. $O_M/P \simeq L(\infty Q)/P \cap L(\infty Q)$ by [9, Prop. III.2.9]. □

Corollary 4.8:

$$N(R) \leq N(L(\infty Q)) + \sum_{M\in \mathrm{MSpec}(R)} \delta_M.$$

□

Table 1 Dimension and redundancy of codes on the curves in Example 4.1.

d	2	3	4	5	6	$7 \leq d \leq 64$
k_1	68	66	64	62	62	$67-d$
k_2	66	64	63	62	61	$67-d$
n_1-k_1	1	3	5	7	7	$d+2$
n_2-k_2	1	3	4	5	6	d

Table 2 Information rate and relative distance of the codes on the curves in Example 4.1.

d	2	3	4	5	6
k_1/n_1	0.9855	0.9565	0.9275	0.8986	0.8986
k_2/n_2	0.9851	0.9552	0.9403	0.9254	0.9104
d/n_1	0.0290	0.0435	0.0580	0.0725	0.0870
d/n_2	0.0300	0.0448	0.0600	0.0746	0.0896

Theorem 4.9: We assume that R is a proper subring of $L(\infty Q)$ and $4G(R)+1 \leq N(R)$ which implies $4G(L(\infty Q))+1 \leq N(L(\infty Q))$. Let $n_1 = N(R)$ and $n_2 = N(L(\infty Q))$ be the code length of $C(R,d)$ and $C(L(\infty Q),d)$ respectively. Let k_1 and k_2 be the dimension of $C(R,d)$ and $C(L(\infty Q),d)$ respectively. Then for designed minimum distance $2G(R)+1 \leq d \leq \min\{n_1 - 2G(R)+1, n_2 - 2G(L(\infty Q))+1\}$,

$$k_1 \leq k_2, \quad n_1 - k_1 > n_2 - k_2.$$

Proof: $n_1 - k_1 = d + G(R) - 1 > d + G(L(\infty Q)) - 1 = n_2 - k_2$.

$$\begin{aligned} k_1 &= N(R) - G(R) - d + 1 \\ &\leq N(L(\infty Q)) - G(L(\infty Q)) - d + 1 \\ &= k_2. \end{aligned}$$

□

The performance of linear codes constructed on curves given in Example 4.1 is tabulated below.

For $7 \leq d \leq 64$ it is clear that codes on the singular curve are worse than codes on its normalization. For $d \leq 6$ we compare the information rate k_i/n_i for $i = 1, 2$ and the relative distance d/n_i.

For $d \geq 4$ both information rate and relative distance of codes on the normalization is better than codes on the original singular curve. For $d = 2, 3$ which codes are preferable depends on applications.

5. Conclusion and Further Study

We showed that the dimension of codes on a singular curve is smaller than or equals to that of the codes on its normalization and the number of check symbol of the former is larger than the latter in a wide range of designed minimum distance. This implies nonsingular curves are optimal for code construction in a wide range of designed minimum distance.

Thus when we have a singular affine algebraic curve with a unique rational place at infinity, it is desirable to construct algebraic geometry codes on the normalization of the original curve. In the next paper [5] the author clarifies how to do it.

Acknowledgments

The author thanks Prof. Homma, Dept. of Mathematics, Kanagawa Univ. for teaching conductor of O'_M/O_M and δ_M, Mr. Umehara, Dept. of Electrical & Electronic Eng., Tokyo Institute of Technology pointing that the assumption of Lemma 3.8 can be weaken, Dr. Miura at SONY Media Lab. for discussion and Dr. Shibuya and Prof. Sakaniwa, Dept. of Electrical & Electronic Eng., Tokyo Institute of Technology for carefully reading the manuscript and pointed out its shortcomings.

References

[1] D. Eisenbud, "Commutative algebra with a view toward algebraic geometry," volume 150 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1995.
[2] R. Hartshorne, "Algebraic geometry," volume 79 of Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1977.
[3] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1720–1732, Nov. 1995.
[4] R. Matsumoto, "Linear codes on nonsingular curves are better than those on singular curves," IEICE Technical Report IT97-81, March 1998.
[5] R. Matsumoto, "Constructing algebraic geometry codes on the normalization of a singular C_{ab} curve," submitted to IEICE Trans. Fundamentals, 1998.
[6] S. Miura, "Linear codes on affine algebraic varieties," Trans. IEICE, vol.J81-A, no.10, pp.1386–1397, Oct. 1998.
[7] S. Miura, "Linear codes on affine algebraic curves," Trans. IEICE, vol.J81-A, no.10, pp.1398–1421, Oct. 1998.
[8] R. Pellikaan and F. Torres, "On Weierstrass semigroups and the redundancy of improved geometric Goppa codes," submitted to IEEE Trans. Inform. Theory, 1998.
[9] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin, 1993.

Ryutaroh Matsumoto received the B.E. degree in computer science and M.E. degree in information processing from Tokyo Institute of Technology in 1996 and 1998 respectively. He is currently a research student in the Department of Electrical and Electronic Engineering, Tokyo Institute of Technology. His current research interest includes algorithms in commutative algebra and algebraic geometry codes. E-mail: ryutaroh@ss.titech.ac.jp