A Dual of Well-Behaving Type Designed Minimum Distance

Tomoharu SHIBUYA† and Kohichi SAKANIWA†, Regular Members

SUMMARY In this paper, we propose a lower bound for the minimum distance of \([n,k]\) linear codes which are specified by generator matrices whose rows are \(k\) vectors of a given sequence of \(n\) linearly independent vectors over a finite field. The Feng-Rao bound and the order bound give the lower bounds for the minimum distance of the dual codes of the codes considered in this paper. We show that the proposed bound gives the true minimum distance for Reed-Solomon and Reed-Muller codes and exceeds the Goppa bound for some \(L\)-type algebraic geometry codes.

key words: designed minimum distance, Feng-Rao bound, order bound, generalized Hamming weights, algebraic geometry codes

1. Introduction

Various kinds of bounds for the minimum distance of linear codes have been investigated in the history of coding theory. Among them, the Feng-Rao bound is well known as the one for algebraic geometry (AG) codes \([1]\). Recently, the Feng-Rao bound is described as the order bound for the dual of evaluation codes and extended to arbitrary linear codes \([2]\).

Let \(F\) be a finite field and \(n\) a positive integer. We denote by \(B := \{b_1, b_2, \ldots, b_n\}\) a basis of \(F^n\), with the order of \(b_i\)'s in \(B\). For \(u = (u_1, u_2, \ldots, u_n)\) and \(v = (v_1, v_2, \ldots, v_n)\) in \(F^n\), \(u \cdot v\) and \(u * v\) represent \(u \cdot v := \sum_{i=1}^{n} u_i v_i\) and \(u * v := (u_1 v_1, u_2 v_2, \ldots, u_n v_n)\), respectively.

For \(B\) and a subset \(G\) of \(B\) with \(|G| = k\) \((1 \leq k \leq n)\), we define a code \(C(B,G)\) over \(F\) by

\[
C(B,G) := \text{span}\{b : b \in G\}
\]

and its dual by

\[
C^\perp(B,G) := \{v \in F^n : v \cdot b = 0 \text{ for all } b \in G\}.
\]

\(C(B,G)\) (resp. \(C^\perp(B,G)\)) is an \([n,k]\) (resp. \([n,n-k]\)) linear code. We denote by \(d(C)\) the minimum distance of a linear code \(C\). The Feng-Rao bound gives a lower bound for the minimum distance of \(C^\perp(B,G)\) as described in the following.

We let \(b_0 := 0\) and denote by \(L_\ell\) \((0 \leq \ell \leq n)\) the linear space over \(F\) spanned by \(b_0, b_1, \ldots, b_\ell\) and let \(L_{\ell-1} := \emptyset\). Then we have a chain of \(F\)-linear spaces \(\{0\} = L_0 \subset L_1 \subset \cdots \subset L_{n-1} \subset L_n = F^n\) with \(\dim L_i = i\) \((0 \leq i \leq n)\). We define a map \(\rho : F^n \to \{0,1,\ldots,n\}\) by

\[
\rho(v) = \ell, \quad \text{if } v \in L_\ell \setminus L_{\ell-1}\.
\]

Let \(I := \{1,2,\ldots,n\}\). A pair \((i,j) \in I^2\) is said to be well-behaving (WB) if \(\rho(b_i \ast b_j) < \rho(b_i \ast b_j)\) for all \(u\) and \(v\) with \(1 \leq u \leq i, 1 \leq v \leq j\) and \((u,v) \neq (i,j)\).

Proposition 1 [2, pp.921–922] For \(B\) and \(G\) given as above, let

\[
A_\ell := \{(i,j) \in I^2 : \rho(b_i \ast b_j) = \ell \text{ and } (i,j) \text{ is WB}\},
\]

\(\ell = 1,2,\ldots,n\)

and define

\[
\delta(B,G) := \min\{|A_\ell| : b_\ell \in B \setminus G\}.
\]

Then \(d(C^\perp(B,G)) \geq \delta(B,G)\).

Suppose \(\rho\) is an order function on some \(F\)-algebra \(R\) and \(B\) is a basis of \(F^n\) which corresponds to an \(F\)-basis of \(R\) where the order of \(b_i\)'s in \(B\) is determined by \(\rho\) and \(G\) consists of the first \(k\) elements of \(B\). Then \(C(B,G)\) becomes an evaluation code and \(\delta(B,G)\) is the order bound for \(d(C^\perp(B,G))\) (see [2]).

For given \(B\) and an integer \(d\), let

\[
G' := \{b_\ell : B : |A_\ell| < d\}.
\]

Then it follows from Proposition 1 that \(d(C^\perp(B,G')) \geq \delta(B,G') \geq d\) [2, Proposition 4.23]. Moreover, it can be shown that if \(\delta(B,G) = d\), then \(C^\perp(B,G') \supset C^\perp(B,G)\) for all \(G \subset B\) with \(\delta(B,G) = d\) [2, Remark 4.25]. This means that for fixed \(B\) and \(d\), the number of check symbols of \(C^\perp(B,G')\) is \(|G'|\) and the smallest among all codes \(C^\perp(B,G)\) with \(\delta(B,G) = d\). This idea to define \(G'\) as above comes from the improved geometric Goppa codes for \(C^\perp(B,G)\) [4].

Instead of \(C^\perp(B,G)\), we introduce in this paper a lower bound for the minimum distance of \(C(B,G)\) by using the map \(\rho\) and the concept of well-behaving. It is true that if we construct a basis of \(F^n\) and its subset, denoted by \(\hat{B}\) and \(\hat{G}\) \((|\hat{G}| = n-|G|)\) respectively, such that

\[
V \setminus W := V \cap W^c = \{a \mid a \in V \text{ and } a \notin W\}.
\]
$C(B,G)$ is expressed as $C_{\perp}(\hat{B}, \hat{G})$, then $d(C(B,G))$ can be estimated by $\delta(B, \hat{G})$, i.e., the Feng-Rao bound for $d(C_{\perp}(\hat{B}, \hat{G}))$. This approach is seen in [3] for one point AG codes. On the other hand, our bound does not require an intermediate set of vectors like $B$ and $\hat{G}$, but can be calculated directly from $B$ and $G$. We also clarify how to choose an optimum $G$ in $B$ for which the dimension of $C(B,G)$ becomes maximum by imitating the construction of improved geometric Goppa codes for $C_{\perp}(B,G)$.

2. A Lower Bound for $d(C(B,G))$

2.1 Main Theorem

In this section, we give the following theorem. We fix $B$ and $G \subset B$ and let $k := |G|$.

Theorem 1 For given $B$ and $G$, let

$$B'_i := \{ \ell : \rho(b_i \ast b_j) = \ell \text{ for some } b_j \in B \text{ s.t. } (i, j) \text{ is WB} \}.$$ 

and $B_i := \{ \nu : b_\nu \in B \setminus G \} \setminus B'_i (i = 1, 2, \ldots, n)$. Define

$$t(B,G) := \max \{|B_i| : b_i \in G \}.$$ 

Then $d(C(B,G)) \geq n - k + 1 - t(B,G)$. □

In order to show Theorem 1, we use some results on the generalized Hamming weights of codes. We denote the support of $v = (v_1, v_2, \ldots, v_n) \in F^n$ by $\text{supp}(v) := \{i : v_i \neq 0\}$, and the support of a subset $A \subset F^n$ by $\text{supp}(A) := \cup_{\nu \in A} \text{supp}(v)$. We also denote by $D_t$ the set of all $t$-dimensional subspaces of $C$.

Definition 1 [5] For an $[n, k]$ linear code $C$, the $t$-th generalized Hamming weight $d_t(C)$ of $C$ is defined as $d_t(C) := \min \{|\text{supp}(D)| : D \in D_t \}$ ($t = 1, 2, \ldots, k$).

The following propositions for the generalized Hamming weights are well known.

Proposition 2 [5], [6] Let $C$ be an $[n, k]$ linear code. Then $d_t(C) < d_{t+1}(C)$ for $t = 1, 2, \ldots, k - 1$. □

Proposition 3 [5], [6] For the generalized Hamming weights of an $[n, k]$ code $C$ and its dual $C_{\perp}$,

$$d_t(C_{\perp}) := \begin{cases} 1 \leq t \leq n-k \{n+1-d_t(C) : 1 \leq t \leq k \} \\ \cup \{n+1-d_t(C) : 1 \leq t \leq k \} = \{1, 2, \ldots, n\}. \end{cases}$$ □

It is obvious from Proposition 3 that $\{d_t(C_{\perp}) : 1 \leq t \leq n-k\}$ and $\{n+1-d_t(C) : 1 \leq t \leq k\}$ are disjoint.

Proposition 4 [5], [6] Let $C$ be an $[n, k]$ linear code.

1. $d_t(C) \leq n-k+t$ for $t = 1, 2, \ldots, k$.

2. If $d_{t'}(C) = n-k+t'$ for some $t'$, then $d_t(C) = n-k+t$ for all $t$ with $t' \leq t \leq k$. □

Inequality given in Proposition 4-(1) is called the generalized Singleton bound for $d_t(C)$, and a code $C$ which satisfies the equality in this bound is called a $t$-th rank maximum distance separable (MDS) code [5].

For an $[n, n-k]$ linear code $C_{\perp}(B,G)$, the minimum value of $t'$ in Proposition 4-(2), that is, the minimum value of $t$ for which $C_{\perp}(B,G)$ becomes a $t$-th rank MDS code, can be estimated by the following proposition.

Proposition 5 $d_t(C_{\perp}(B,G)) = k + t$ for all $t$ with $t(B,G) + 1 \leq t \leq n-k$. □

This proposition was first shown for $G = \{b_1, b_2, \ldots, b_k\}$ [7, Theorem 2] while it can be proven for an arbitrary subset $G$ of $B$ with $|G| = k$, and plays an important role to connect $t(B,G)$ with $d(C(B,G))$. The proof of this proposition is rather long and shall be given in the next subsection.

(Proof of Theorem 1)

For simplicity, we denote $C(B,G)$ by $C$.

We have from Proposition 2 that $\max\{n+1-d_t(C) : 1 \leq t \leq k\} = n+1-d_1(C) = n+1-d(C)$. Thus

Proposition 3 yields that $n+1-d(C) \not\in \{d_t(C_{\perp})\}_{t=1}^{n-k}$ and $\{\ell : n+2-d(C) \leq \ell \leq n\} \subset \{d_t(C_{\perp})\}_{t=1}^{n-k}$. Therefore we have

$$d_t(C_{\perp}) \begin{cases} < k + t, 1 \leq t \leq n - k - d(C) + 1, \\ = k + t, n - k - d(C) + 2 \leq t \leq n - k. \end{cases} \quad (1)$$

By comparing the second relation of Eq.(1) and the relation given in Proposition 5, we have $t(B,G) + 1 \geq n - k - d(C) + 2$, that is $d(C) \geq n - k + 1 - t(B,G)$. □

Now let us consider how to choose an optimum $G \subset B$ for which the dimension of $C(B,G)$ becomes maximum. For given $B$ and an integer $\tau$, let $G' := \{b_i : |B_i| \leq \tau\}$.

Then we have from the definitions of $G'$ and $t(B,G)$ that $t(B,G') \leq \tau$ and therefore $d(C(B,G')) \geq n - k + 1 - \tau$ by Theorem 1. Moreover it is obvious from the definitions of $G'$ and $t(B,G)$ that if $t(B,G') = t(B,G)$ then $G \subset G'$. Thus if $t(B,G') = \tau$, then $C(B,G') \supset C(B,G)$ for all $G \subset B$ with $t(B,G) = \tau$. This means that for fixed $B$ and $\tau$, the dimension of $C(B,G')$ is $|G'|$ and the largest among all codes $C(B,G)$ with $t(B,G) = \tau$.

Remark 1 A pair $(i,j) \in I^2$ is said to be weakly well-behaving (WWB) if $\rho(b_i \ast b_j) < \rho(b_i \ast b_j)$ for all $u$ with $1 \leq u < i$ and $\rho(b_i \ast b_j) < \rho(b_i \ast b_j)$ for all $v$ with $1 \leq v < j$ [8]. It has been shown that Proposition 1 still holds for $A_e$ defined by using WWB in place of WB [8]. Since WWB pair $(i,j)$ is also WWB, the lower bound $\delta(B,G)$ can be improved by employing the notion of WWB.
It is also shown that we can replace WB by WWB in Theorem 1 and can improve the proposed bound \( n - k + 1 - t(B,G) \). In Remark 2 at the end of the next subsection, it will be argued that Proposition 5 replaced WB by WWB also holds, which shows that so does Theorem 1 with WWB in place of WB.

2.2 Proof of Proposition 5

The proof of Proposition 5 consists of two parts. At first, we establish a lower bound for \( d_i(C^-(B,G)) \). Once we derive the lower bound, we can describe a condition on \( t \) under which the established lower bound agrees with the generalized Singleton bound by using the parameter \( t(B,G) \).

In this subsection, we denote by \( D \) the set of all \( t \)-dimensional subspaces of \( C^-(B,G) \). In order to refer to the set of indices of elements in \( G \), let \( I := \{1,2,\ldots,n\} \) and define \( I(G) := \{i : i \in I \subseteq G \} \).

For given \( D \in D_t \), we define an \( F \)-linear map \( \theta_D : F^n \to F^n \), \( \nu = (v_1, v_2, \ldots, v_n) \mapsto \nu^D := \theta_D(\nu) = (v_1^D, v_2^D, \ldots, v_n^D) \) by

\[
v_i^D := \begin{cases} v_i, & \text{if } i \in \text{supp}(D), \\ 0, & \text{if } i \not\in \text{supp}(D). \end{cases}
\]

Then define \( W^0 := \theta_D(W) = \{u^\nu : u \in W\} \) for a linear subspace \( W \subset F^n \). By the definition of \( L_\ell, L_D^0 \) becomes the linear span of \( b_0^\nu, b_1^\nu, \ldots, b_n^\nu \), and therefore \( (F^n)^0 = L_n^0 \). Since \( |\text{supp}(D)| = \dim(F^n)^0 \), we have

\[
|\text{supp}(D)| = \dim L_n^0. \tag{2}
\]

Moreover, by noting that \( \{b_i^\nu : i \in I, b_i^\nu \not\in L_{i-1}^0\} \) becomes a basis of \( L_{i-1}^0 \), Eq.(2) yields

\[
|\text{supp}(D)| = |\{b_i^\nu : i \in I, b_i^\nu \not\in L_{i-1}^0\}| = |\{i : i \in I \setminus I(G), b_i^\nu \not\in L_{i-1}^0\}| + |\{i : i \in I(G), b_i^\nu \not\in L_{i-1}^0\}| \tag{3}
\]

In the following, we shall give lower bound for each term of Eq.(3) which holds for any \( D \in D_t \). Then we establish a lower bound for \( |\text{supp}(D)| \) for any \( D \in D_t \), that is, a lower bound for \( d_i(C^-(B,G)) \).

For a linear subspace \( W \subset F^n \), we consider the linear subspace \( W^\perp \subset F^n \) defined by

\[
W^\perp := \{\nu \in F^n : \text{supp}(\nu) \subset \text{supp}(D) \text{ and } \nu \cdot u = 0 \text{ for all } u \in W\}.
\]

Then we have

\[
\dim L_n^0 = \dim W^D + \dim(W^D)^\perp \tag{4}
\]

for any \( D \in D_t \).

Since \( D \in D_t \) satisfies \( D \subset C^-(B,G) \), for all \( c = (c_1, c_2, \ldots, c_n) \in D \) and \( b_i = (b_{i1}, b_{i2}, \ldots, b_{in}) \in G \), we have

\[
0 = c \cdot b_i = \sum_{j=1}^{n} c_j b_{ij} = \sum_{j \in \text{supp}(D)} c_j b_{ij} = c_i^D \cdot b_i^D
\]

which implies that

\[
D \subset (C(B,G)^0)^\perp. \tag{5}
\]

The following lemma gives a lower bound for the first term of Eq.(3).

Lemma 1 For any \( D \in D_t \), \( \{|i : i \in I \setminus I(G), b_i^\nu \not\in L_{i-1}^0\} \geq t \).

(proof) For simplicity, we denote \( C(B,G) \) by \( C \).

Let

\[
U := \{b_i^\nu : i \in I, b_i^\nu \not\in L_{i-1}^0, b_i^\nu \in C^D\},
\]

\[
V := \{b_i^\nu : i \in I, b_i^\nu \not\in L_{i-1}^0, b_i^\nu \not\in C^D\}.
\]

Then \( U \cap V = \emptyset \) and for any \( D \in D_t \),

\[
L_n^0 = \langle b_i^\nu : i \in I, b_i^\nu \not\in L_{i-1}^0 \rangle = \langle U \rangle \oplus \langle V \rangle \tag{6}
\]

where \( \oplus \) denotes direct sum. Since \( \langle U \rangle \subset C^D \), we have

\[
t = \dim \langle U \rangle \leq \dim C^D \tag{7}
\]

Finally, for \( b_i \in B \), if \( b_i^\nu \not\in C^D \) then \( b_i \not\in C \) and therefore \( i \in I \setminus I(G) \) which implies that for any \( b_i^\nu \in V \), \( i \in I \setminus I(G) \) and \( b_i^\nu \not\in L_{i-1}^0 \). Then the lemma follows.

In order to derive a lower bound for the second term of Eq.(3), we need some preliminary lemmas.

Lemma 2 Let \( (i,j) \in I^2 \) be well-behaving and \( \ell := \rho(b_i \ast b_j) \). For given \( D \in D_t \), if \( b_i^\nu \in L_{i-1}^0 \) or \( b_j^\nu \in L_{j-1}^0 \), then \( b_i^\nu \ast b_j^\nu \in L_{\ell-1}^0 \).

(proof) Since \( b_i \ast b_j \) can be expressed as \( b_i \ast b_j = \sum_{\nu=1}^{\ell} \alpha_{\nu} b_{\nu} \) with \( b_{\nu} \in B \), \( \alpha_{\nu} \in F \) and \( \alpha_{\ell} \not= 0 \), \( \theta_D(b_i \ast b_j) = b_i^\nu \ast b_j^\nu \) is expressed as

\[
b_i^\nu \ast b_j^\nu = \sum_{\nu=1}^{\ell} \alpha_{\nu} b_{\nu}, \ b_{\nu} \in B, \alpha_{\nu} \in F, \alpha_{\ell} \not= 0. \tag{8}
\]

We assume without loss of generality that \( b_i^\nu \in L_{i-1}^0 \). Then \( b_i^\nu \ast b_j^\nu \) can be expressed in a different way as

\[
b_i^\nu \ast b_j^\nu = \left( \sum_{u=1}^{i-1} \beta_u b_u^\nu \right) \ast b_j^\nu = \sum_{u=1}^{i-1} \beta_u b_u^\nu \ast b_j^\nu
\]

Since \( (i,j) \) is well-behaving, \( \rho(b_u \ast b_j) \leq \ell \) for every \( 0 \leq u \leq i - 1 \). Hence

\[
b_i^\nu \ast b_j^\nu = \sum_{\nu=1}^{\ell-1} \gamma_{\nu} b_{\nu}^\nu, \ b_{\nu} \in B, \gamma_{\nu} \in F. \tag{9}
\]
Lemma 3 For $D \subset D_1$, we define $T_D := \{ i : i \in I(G), b_i^o \in L_{i-1}^o \}$. For any $b_i$ with $\ell \in I \setminus I(G)$, if $b_i^o \not\in L_{i-1}^o$, then $\ell \not\in B_{T_D}$.

(proof) We show the contraposition. For any $\ell \in B_{T_D} = \bigcup_{i \in T_D} B_i'$, there exists some $i \in T_D$ such that $\ell \in B_i'$. Therefore, by the definition of $B_i'$, there exists some $b_j \in B$ such that $\ell = \rho(b_j * b_j)$ and $(i, j)$ is well behaving.

On the other hand, by the definition of $T_D$, $b_i^o \in L_{i-1}^o$ for any $i \in T_D$. Thus by Lemma 2 we have $b_i^o \in L_{i-1}^o$. \hfill $\square$

The following lemma provides a lower bound for the second term of Eq.(3).

Lemma 4 For an $[n, n-k]$ code $C^+(B, G)$, let

$$\eta_t := \max\{|T| : T \subset I(G) \setminus B_{T_D} \} \quad \text{s.t.} \quad |\{ i : i \in I \setminus I(G) \} \setminus B_{T_D}'| \geq t. \quad (9)$$

Then $|\{ i : i \in I(G), b_i^o \not\in L_{i-1}^o \}| \geq k - \eta_t$ for any $D \subset D_1$.

(proof) Note that we have defined $T_D := \{ i : i \in I(G), b_i^o \in L_{i-1}^o \}$, which yields

$$|\{ i : i \in I(G), b_i^o \not\in L_{i-1}^o \}| = |I(G)| - |T_D| = k - |T_D|.$$

Thus it is sufficient to show that $|T_D| \leq \eta_t$ holds.

For each $i \in I \setminus I(G)$, if $b_i^o \not\in L_{i-1}^o$ then $i \not\in B_{T_D}$ by Lemma 3, which means

$$\{ i : i \in I \setminus I(G), b_i^o \not\in L_{i-1}^o \} \subset \{ i : i \in I \setminus I(G) \} \setminus B_{T_D}'. \quad (10)$$

Thus we see from Lemma 1 and Eq.(10) that $|\{ i : i \in I \setminus I(G) \} \setminus B_{T_D}'| \geq t$ for any $D \subset D_1$. Moreover, by noting that $T_D \subset I(G)$, we have

$$\{ T_D : D \subset D_1 \} \subset \{ T \subset I(G) : |\{ i : i \in I \setminus I(G) \} \setminus B_{T_D}'| \geq t \}.$$
Definition 2 [2, Example 4.18] The q-ary Reed-Muller (RM) code of order u and in m variables is defined by $\text{RM}_q(u, m) := \{\psi(f) : f \in R, \deg(f) \leq u\}$. □

A monomial $f_i = \prod_{\ell=1}^{m} X_{\ell}^{i_{\ell}} \in R$ is said to be reduced if $0 \leq i_{\ell} \leq q - 1$ for all $\ell (1 \leq \ell \leq m)$. Denote by $M$ the set of all reduced monomials in $R$. Then $|M| = q^m (= n)$ and it is shown in [9] that $\text{RM}_q(u, m) = \text{span}(\psi(f) : f \in M, \deg(f) \leq u)$. Write $M = \{f_1, f_2, \ldots, f_n\}$ with $f_i < f_{i+1}$, where $<$ denotes an order relation. We here employ the order relation defined by:

for $f_i = \prod_{\ell=1}^{m} X_{\ell}^{i_{\ell}}$ and $f_j = \prod_{\ell=1}^{m} X_{\ell}^{j_{\ell}}$ in $M$, $f_i \prec f_j$ if (i) $\deg(f_i) < \deg(f_j)$, or (ii) $\deg(f_i) = \deg(f_j)$ and $f_i <_L f_j$, where $<_L$ denotes a lexicographic order [10], i.e., $f_i <_L f_j$ if there exists a nonzero entry in the vector $(j_1 - i_1, j_2 - i_2, \ldots, j_m - i_m)$ and the left-most nonzero entry is positive.

Moreover, it is well known that $\text{RM}_q(u, m) = \text{RM}_q(m(q - 1) - u - 1, m)$ [9, Remark 4.7].

For RM codes $\text{RM}_q(u, m) = C(B, G)$, $t(B, G)$ is expressed as in the following proposition.

Proposition 6 [7, Theorem 4] For $\text{RM}_q(u, m) = C(B, G)$ where $B$ and $G$ are given as above with $k := |G|$, let $Q$ and $R$ be integers such that

$$u = Q(q - 1) + R; \ 0 \leq Q, \ 0 \leq R \leq q - 2.$$ (12)

Then $t(B, G) = q^m - k - (q - R)q^{m-(Q+1)} + 1$. □

By noting that $q^m = n$, we have from Proposition 6 and Theorem 1 that

$$d(\text{RM}_q(u, m)) \geq n - k + 1 - t(B, G)\quad = (q - R)q^{m-(Q+1)}.$$ On the other hand, we can easily show that $d(\text{RM}_q(u, m)) = (q - R)q^{m-(Q+1)}$, which implies that the bound given in Theorem 1 gives the true minimum distance for RM codes.

Moreover, by substituting $d(\text{RM}_q(u, m)) = n - k + 1 - t(B, G)$ for $d(C)$ in Eq.(1), we see that for RM codes, $d(C_{\perp}) = k + t$ if and only if $t(B, G) + 1 \leq t \leq n - k$. This assertion is stronger than Proposition 5.

3.3 Algebraic Geometry Codes

In this subsection, the terminology follows [11]. Let $F_q := GF(q)$ and $F/F_q$ be an algebraic function field of genus $g$. We denote by $P_1, \ldots, P_n$ pairwise distinct places of $F/F_q$ of degree one and $D := P_1 + \cdots + P_n$. Moreover, let $E$ be a divisor of $F/F_q$ such that $\text{supp}(E) \cap \text{supp}(D) = \emptyset$. For the divisor $E$, we define an $F_q$-linear space by $L(E) := \{f \in F : (f) + E \geq 0\} \cup \{0\}$. For the divisor $D$, we define an $F_q$-linear map $\phi_D : L(E) \rightarrow F_q^n$ by $\phi_D(f) := (f(P_1), f(P_2), \ldots, f(P_n))$. Then we can define an algebraic geometry (AG) code associated with the divisors $D$ and $E$ by $C_L(D, E) := \text{Im}(\phi_D)$.

Now we consider AG codes on the function field $F_q(x,y)/F_q$ with $c_0x^b + c_{0,a}y^a + p(x,y) = 0$ where $\gcd(a,b) = 1$ and

$$p(x,y) = \sum_{0 < i,j < ab} c_{i,j} x^iy^j,$$

$c_{i,j} \in F_q, c_{0,0} \neq 0, c_{0,a} \neq 0.$

This equation is known as $C_{ab}$ curve [12] and we assume that it is non-singular and absolutely irreducible. In this case the genus of $F_q(x,y)/F_q$ is $g = (a-1)(b-1)/2$.

Let $Q$ be the common pole of $x$ and $y$ and consider a one point AG code $C_L(D, E) := C_L(D, mQ)$. We denote by $f_1, f_2, \ldots, f_t$ ($t := \dim(L(mQ))$) a basis of $L(mQ)$ with $v_Q(f_i) > v_Q(f_{i+1})$ where $v_Q$ denotes a discrete valuation at $Q$. Next we consider a subset of $\{f_1, f_2, \ldots, f_t\}$ defined by

$$\{f_i : \phi_D(f_i) \notin \text{span}\{\phi_D(f_1), \ldots, \phi_D(f_{i-1})\}\}.$$

It is known that for a sufficiently large $m$, $\phi_D(L(mQ)) = F_q^n$ and therefore the cardinality of this subset is $n$. Hence we can express this subset as $\{g_1, g_2, \ldots, g_n\}$ and $\{\phi_D(g_1), \phi_D(g_2), \ldots, \phi_D(g_n)\}$ becomes a basis of $F_q^n$. Let $B := \{b_1, b_2, \ldots, b_n\}$ with $b_i := \phi_D(g_i)$ and $G := \{b_i : v_Q(g_i) \geq -m\}$. Then $C_L(D, mQ) = C(B, G)$.

It is known that $C_L(D, E)$ is an $[n,k,d]$ code with $d \geq n - k + 1 - g$ [11, Corollary II.2.3], where $k := \dim(L(E))$ and $g$ is the genus of the algebraic function field. $n - k + 1 - g$ is known as the Goppa bound for $C_L(D, E)$. On the other hand, we have shown that $t(B, G) \leq g$ holds [7, Theorem 5] when we define $B$ and $G$ for one point AG codes on $C_{ab}$ curve as explained above. Thus we can conclude that the bound given in Theorem 1 can be better than the Goppa bound.

Lower bounds for the minimum distance of one point AG codes are also investigated in [2] and [3]. In [2], one point AG codes are regarded as a special case of evaluation codes [2, Remark 4.4] and the lower bound for the minimum distance agrees with the Goppa bound [2, Corollary 5.19]. Hence, at least for one point AG

$\#(m(q - 1) - u = \nu(q - 1) + \mu, \ 0 \leq \nu, \ 0 \leq \mu \leq q - 2.$ (13)

By adding Eq.(12) and Eq.(13), we have $(m - (Q + \nu))(q - 1) = R + \mu$.

If $R + \mu = 0$, we have $R = 0 = \mu$ because $R, \mu \geq 0$ and therefore $Q = m - \nu$. On the other hand, if $R + \mu \neq 0$, by noting that $0 \leq R + \mu \leq 2(q - 2)$, we have $R + \mu = q - 1$ and therefore $m - (Q + \nu) = 1$. In either case, we have $(q - R)q^{m-(Q+1)} = (\mu + 1)q^\nu (= d(\text{RM}_q(u, m)))$. 

$\Box$
codes on $C_{ab}$ curves, Theorem 1 gives a better bound than that given in [2].

On the other hand, it is guaranteed that the lower bound given in [3] is greater than or equal to the Goppa bound. In Sect. 4 of [3], numerical values of their lower bound for the minimum distance of an AG code constructed on an algebraic function field discovered in [13] have been calculated. If one applies Theorem 1 to this AG code, he will find numerically that the lower bound given in Theorem 1 agrees with that given in [3]. For other (one point) AG codes, relations between these two bounds are left for further study.

4. Conclusion

In this paper, we have proposed a lower bound for the minimum distance of $C(B, G)$ which is expressed by the map $\rho$ and the concept of well-behaving. We have also proposed the construction method of $G \subset B$ for given $B$ and $\tau$ for which the dimension of $C(B, G)$ is the largest among all codes with $t(B, G) = \tau$. Moreover, we have shown that the proposed bound gives the true minimum distance for Reed-Solomon and Reed-Muller codes and exceeds the Goppa bound for one point algebraic geometry codes on an algebraic function field defined by a $C_{ab}$ curve.

As for $C^\perp(B, G)$, $\delta(B, G)$ is deeply related to its decoding algorithm, so called Feng-Rao algorithm. Thus it is a further study to investigate relations between $t(B, G)$ and a decoding algorithm for $C(B, G)$.

Acknowledgment

The authors are grateful to Mr. R. Matsumoto for providing a complete numerical data given in [3]. They also wish to thank Mr. R. Hasegawa for his useful discussion.

References


Tomoharu Shibuya received the B.E., M.E., and Ph.D. degrees in electrical and electronic engineering from Tokyo Institute of Technology, Tokyo, Japan, in 1992, 1994 and 1999, respectively. He joined Tokyo Institute of Technology in 1994 as a research associate. Since 2000, he has bee a research associate in the Department of Communication and Integrated Systems, Graduate School of Science and Engineering, Tokyo Institute of Technology. His research interests are error control coding and information theory.

Kohichi Sakaniwa received B.E., M.E., and Ph.D. degrees all in electronic engineering from the Tokyo Institute of Technology, Tokyo Japan, in 1972, 1974 and 1977, respectively. He joined the Tokyo Institute of Technology in 1977 as a research associate and served as an associate professor from 1983 to 1991. Since 1991 he has been a professor in the Department of Electrical and Electronic Engineering, and since 2000 in the Department of Communication and Integrated Systems, Graduate School of Science and Engineering, both in the Tokyo Inst. of Tech. He received the Excellent Paper Award from the IEICE (the Institute of Electronics, Information and Communication Engineers) of Japan in 1982, 1990, 1992 and 1994. His research area includes Communication Theory, Error Correcting Coding, (Adaptive) Digital Signal Processing and so on. Dr. Sakaniwa is a member of IEEE, IEICE Japan, Information Processing Society of Japan, Institute of Image Information and Television Engineers of Japan, Society of Information Theory and its Applications, and Institute of Electronic Engineers of Japan.