AN MDS CODE ASSOCIATED TO AN ELLIPTIC CURVE

KEN-ICHI SUGIYAMA

Department of Mathematics and Informatics,
Faculty of Science, Chiba University.
1-33 Yayoi-cho Inage-ku, Chiba
263-8522, Japan
e-mail address: sugiyama@math.s.chiba-u.ac.jp

Abstract. We will construct an MDS (= the most distance separable) code \( C \) which admits a decomposition \( C = \oplus_i C_i \) such that every factor is still MDS. An effective way of decoding will be also discussed.

Keywords: algebraic geometry; Goppa codes; elliptic curves; MDS codes
2010 Mathematical Subject Classification: 11T71, 14G50, 94B27.

1. Introduction

Let \( q \) be a power of a prime \( p \). A code \( C \) is an imbedding
\[
e : C \rightarrow \mathbb{F}_q^N, \quad N \geq 1,
\]
where \( C \) is a vector space over \( \mathbb{F}_q \) and the minimal distance \( d(C) \) is defined to be one of \( e(C) \), that is
\[
d(C) := \text{Min}_{x \neq 0 \in e(C)} w(x),
\]
where \( w(x) \) is the weight of the cordwood \( x = (x_1, \ldots, x_N) \), i.e. the number of non-zero \( x_i \). It is known \( d(C) \leq N - \dim C + 1 \) by the Singleton bound and if the equality hold the code is called MDS\(^*(I)\) Chapter 11. If \( d(C) \geq N - \dim C \), we mention \( C \) as NMDS\(^†\).

A MDS or NMDS code has been naturally appeared in various references. Let \( E \) be an elliptic curve defined over \( \mathbb{F}_q \) and \( \Sigma = \{s_1, \ldots, s_N\} \) a subset of \( E(\mathbb{F}_q) \), the set of \( \mathbb{F}_q \)-rational points. We identify the space \( \mathbb{F}_q^\Sigma \) of \( \mathbb{F}_q \)-valued functions on \( \Sigma \) with \( \mathbb{F}_q^N \) by
\[
\mathbb{F}_q^\Sigma \cong \mathbb{F}_q^N, \quad f \mapsto (f(s_1), \ldots, f(s_N)).
\]
Let \( D \) be a non-zero effective divisor on \( E \) defined over \( \mathbb{F}_q \) whose support \( \text{Spt}(D) \) is disjoint from \( \Sigma \). Then we have the evaluation map,
\[
e : \mathcal{L}(D) \rightarrow \mathbb{F}_q^\Sigma, \quad e(f)(s) = f(s) \quad (s \in \Sigma).
\]
Here \( \mathcal{L}(D) := \{ f \in \mathbb{F}_q(E) | \text{div}(f) + D \geq 0 \} \), where \( \mathbb{F}_q(E) \) is the space of rational functions on \( E \) over \( \mathbb{F}_q \). According to a situation, we will often denote it by \( H^0(E, \mathcal{O}(D)) \), which is a notation of algebraic geometry. The map \( e \) is injective if \( N > \deg(D) \) and
we assume it in the following. Then (2) is an NMDS code with \( \dim \mathcal{L}(D) = \deg(D) \) and is denoted by \( \mathcal{C}_L(D, \Sigma) \). It is MDS iff for every subset \( X \) of \( \Sigma \) with \( |X| = \deg(D) \) the divisor \( D - (X) \) is not principal, where \( (X) := \sum_{x \in X} x \in \text{Div}(E) \) and \( |\cdot| \) is the cardinality\( (3) \). Fix \( P \in \Sigma \) and set \( \Sigma^* := \Sigma \setminus P \). We define \( \mathcal{L}_0(D) \) to be

\[
\mathcal{L}_0(D) = \{ f \in \mathcal{L}(D) \mid f(P) = 0 \}.
\]

Since the space of constant functions \( \mathbb{F}_q \) is contained in \( \mathcal{L}(D) \), \( \dim \mathcal{L}_0(D) = \dim \mathcal{L}(D) - 1 \) and one see that the code \( \mathcal{C}^0_L(D, \Sigma^*) \) defined by

\[
e^* : \mathcal{L}_0(D) \to \mathbb{F}_q^{\Sigma^*}, \quad e(f)(s) = f(s) \quad (s \in \Sigma^*),
\]

is NMDS. Moreover it is MDS if so is \( \mathcal{C}_L(D, \Sigma) \) (cf. Lemma 2.1).

Suppose that the code (1) is NMDS (resp. MDS). A decomposition \( \mathcal{C} = \oplus_i \mathcal{C}_i \) is mentioned as proper if the restriction

\[
e : \mathcal{C}_i \to \mathbb{F}_q^N,
\]

is also NMDS (resp. MDS) for each \( i \).

Set \( k = \mathbb{F}_q \) and \( k_m = \mathbb{F}_{q^m} \) for a positive integer \( m \). Fix a positive square free integer \( N \) and let \( \mathcal{D}(N) \) describe the set of divisors of \( N \). Let \( E \) be an elliptic curve defined over \( k \). Take a prime \( l \neq p \) and we consider a representation

\[
\rho_l : \text{End}_k(E) \to \text{End} T_l(E),
\]

where \( T_l(E) \) is the \( l \)-adic Tate module. Let \( F \) be the \( q \)-th power endomorphism of \( E \) and \( \alpha \) an eigenvalue of \( \rho_l(F) \), which is an algebraic integer with modulus \( \sqrt{q} \). For a positive integer \( n \) we put

\[
(x)_n = \sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1},
\]

and denote the set of primes dividing \( n \) by \( P(n) \).

**Theorem 1.1.** Let \( E \) be an elliptic curve over \( k \) and \( N \) a positive square free integer. Then there are effective divisors \( D_N \) and \( \{D_r\}_{r \in P(N)} \) defined over \( k_N \) which satisfies the following properties.

1. \( D_r \leq D_N, \quad \forall r \in P(N) \).
2. There is a decomposition

\[
\mathcal{L}_0(D_N) = \oplus_{r \in P(N)} \mathcal{L}_0(D_r),
\]

and the projector to the \( r \)-th factor \( \phi^0_{N/r} \) is explicitly described.
3. \( \dim \mathcal{L}_0(D_r) = |(\alpha)_r|^2 - 1, \quad \forall r \in P(N), \)

and in particular

\[
\dim \mathcal{L}_0(D_N) = \sum_{r \in P(N)} |(\alpha)_r|^2 - 1.
\]
Lemma 2.1. Let $D_N$ be a nonzero effective divisor whose support is disjoint from $\Sigma$. If $|\Sigma| > \deg(D)$, $C^0_L(D, \Sigma^*)$ is NMDS. If moreover $C_L(D, \Sigma)$ is MDS, so is $C^0_L(D, \Sigma^*)$.

Proof. We first claim that $e^*: \mathcal{L}_0(D) \to k^{\Sigma^*}$ is injective. We define $e_P: \mathcal{L}(D) \to k$, $e_P(s) = s(P)$,

In order to construct a code we take a finite subset $\Sigma$ of $E$ disjoint from the support of $D_N$ with $|\Sigma| > \deg(D_N)$. In fact we can take such a subset in $E(k_N) \setminus \text{Spt}(D_N)$ (cf. Lemma 4.1). Then $C^0_L(D_N, \Sigma^*)$ is automatically NMDS defined over $k_N$ and the decomposition of Theorem 1.1 (2) is proper. In order to obtain an MDS code which admits a proper decomposition the construction of $\Sigma$ is rather involved.

Theorem 1.2. Let $D_N$ and $\{D_r\}_{r \in P(N)}$ be effective divisors in Theorem 1.1 and take an arbitrary integer $m$ greater than $\deg(D_N)$. Then there is a subset $\Sigma$ of $E(k_N^{'})$ ($k_N^{'}$ is a finite extension of $k_N$) which satisfies the following properties.

1. $\Sigma$ is disjoint from the support of $D_N$ and $|\Sigma| = m$.
2. All the codes $C^0_L(D_N, \Sigma^*)$ and $\{C^0_L(D_r, \Sigma^*)\}_{r \in P(N)}$ are MDS. In particular the decomposition

$$\mathcal{L}_0(D_N) = \oplus_{r \in P(N)} \mathcal{L}_0(D_r),$$

is proper.

We will show a concrete example of Theorem 1.2 in the final section (cf. Theorem 6.1). In general it is not hard to construct a code that admits a proper decomposition from a divisor on an elliptic curve (cf. Proposition 2.1 and Proposition 2.2). But in order to describe $\phi^0_{N/r}$ explicitly we will construct $D_N$ and $\{D_r\}_{r \in P(N)}$ from the kernel of an isogeny of the elliptic curve (cf. Theorem 4.3).

Here is a significance of the theorem. Take a word $w \in \mathcal{L}_0(D_N)$ and let $c := e^*(w) \in k_N^{\Sigma^*}$ be the corresponding code word. We transmit $c$ and let $c'$ be the received vector. Then because of an interference $c' = c + \epsilon$, where $\epsilon$ is an error. If the weight of $\epsilon$ is less than the half of the minimal distance of $C_L(\mathcal{L}_0(D_N), \Sigma^*)$ we can correct errors by the Pellikaan’s algorithm (see §5). Our aim is to find another way which may correct an error of a larger weight. First we decompose $w = \sum_{r \in P(N)} \phi^0_{N/r}(w)$ and we will use the family $\{c_r := e^*(\phi^0_{N/r}(w))\}_r$ as a code word. Transmit them and let $\{c'_r\}_r$ be the received vectors. As before by the Pellikaan’s algorithm we can properly decode $c'_r$ if the weight of the error vector is less than the half of $d(C_L(\mathcal{L}_0(D_r), \Sigma^*))$. Sum them up and then we will recover the original word $w$ if the weight of the error of $c'_r$ is less than the half of $\text{Min}_{r} d(C_L(\mathcal{L}_0(D_r), \Sigma^*))$ for every $r$. Since $\text{Min}_{r} d(C_L(\mathcal{L}_0(D_r), \Sigma^*)) > d(C_L(\mathcal{L}_0(D_N), \Sigma^*))$ we expect that the latter method may correct more errors than the previous (i.e. usual) one.

2. A proper decomposition

Let $E$ be an elliptic curve defined over a finite field $k$ of characteristic $p$. In the following we fix a subset $\Sigma$ of $E(k)$ and a point $P \in \Sigma$. 

Lemma 2.1. Let $D$ be a nonzero effective divisor whose support is disjoint from $\Sigma$. If $|\Sigma| > \deg(D)$, $C^0_L(D, \Sigma^*)$ is NMDS. If moreover $C_L(D, \Sigma)$ is MDS, so is $C^0_L(D, \Sigma^*)$.

Proof. We first claim that $e^*: \mathcal{L}_0(D) \to k^{\Sigma^*}$ is injective. We define $e_P: \mathcal{L}(D) \to k$, $e_P(s) = s(P)$,
and

\[ \nu_P : k^{\Sigma} \to k, \quad \nu_P(f) = f(P), \]

and let \( \epsilon : k^{\Sigma^*} \to k^{\Sigma} \) be the extension by 0 on \( P = \Sigma \setminus \Sigma^* \). Then

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{L}_0(D) & \longrightarrow & \mathcal{L}(D) & \overset{\epsilon_p}{\longrightarrow} & k & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & k^{\Sigma^*} & \overset{\epsilon}{\longrightarrow} & k^\Sigma & \overset{\nu_P}{\longrightarrow} & k & \longrightarrow & 0,
\end{array}
\]

shows that if \( \epsilon \) is injective so is \( \epsilon^* \). Hence the assumption implies the claim. Next we investigate the minimal distance. For a function \( f \) on \( \Sigma \) we set \( \nu(f) := |\Sigma| - w(f) \), that is the number of zeros. Let \( f \neq 0 \in \mathcal{L}_0(D) \) and we have to show that

\[ w(f^*(f)) \geq |\Sigma^*| - \dim\mathcal{L}_0(D) = |\Sigma| - \deg(D). \]

Suppose that \( w(f^*(f)) < |\Sigma| - \deg(D) \). Since \( |\Sigma| - w(f^*(f)) = \nu(f) \), this is equivalent to \( \nu(f) > \deg(D) \) and \( f = 0 \). Hence \( C^0_L(D, \Sigma^*) \) is NMDS. Finally suppose that \( C^0_L(D, \Sigma) \) be an MDS code and let \( g \in \mathcal{L}(D) \). Then \( \nu(g) \geq \deg(D) \) implies \( g = 0 \). If \( f \in \mathcal{L}_0(D) \) satisfies \( w(f^*(f)) \leq |\Sigma^*| - \dim\mathcal{L}_0(D) \), \( \nu(f) \geq \deg(D) \) by the above equations and \( f = 0 \). Therefore \( C^0_L(D, \Sigma) \) is MDS.

\[ \square \]

**Lemma 2.2.** Let \( X \) and \( Y \) be subsets of \( E(k) \) that are disjoint from \( \Sigma \). Suppose that they meet at a single point. Then

\[ \mathcal{L}_0((X \cup Y)) = \mathcal{L}_0((X)) \oplus \mathcal{L}_0((Y)). \]

**Proof.** Let \( Q \) be the intersection of \( X \) and \( Y \). Then

\[ H^0(E, \mathcal{O}(X)) \cap H^0(E, \mathcal{O}(Y)) = H^0(E, \mathcal{O}(Q)) = k, \]

which yields an exact sequence

\[ 0 \to k \to H^0(E, \mathcal{O}(X)) \oplus H^0(E, \mathcal{O}(Y)) \overset{s}{\to} H^0(E, \mathcal{O}(X \cup Y)), \]

where \( s(f, g) = f + g \). Since

\[ \dim H^0(E, \mathcal{O}(X \cup Y)) = |X| + |Y| - 1 = \dim H^0(E, \mathcal{O}(X)) + \dim H^0(E, \mathcal{O}(Y)) - 1, \]

\( s \) is surjective. For a rational function \( f \) regular at \( P \) we define \( e_P(f) := f(P) \) as before and set

\[ \delta(x) = (x, x), \quad \sigma(x, y) = x + y, \quad x, y \in k. \]

Then take the kernels of the vertical arrows of the following diagram and the claim is obtained:

\[
\begin{array}{ccccccccc}
0 & \longrightarrow & k & \longrightarrow & H^0(E, \mathcal{O}(X)) \oplus H^0(E, \mathcal{O}(Y)) & \overset{s}{\longrightarrow} & H^0(E, \mathcal{O}(X \cup Y)) & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \overset{\delta}{\longrightarrow} & k & \overset{\sigma}{\longrightarrow} & k & \longrightarrow & 0.
\end{array}
\]

\[ \square \]
Proposition 2.1. Let \( \{X_i\}_i \) be a finite family of subsets of \( E(k) \) disjoint from \( \Sigma \) which meet at a single point. Then
\[
\mathcal{L}_0((\cup_i X_i)) = \oplus_i \mathcal{L}_0((X_i)).
\]
In general let \( \{Y_i\}_{i \in I} \) be a finite family of subsets of \( E(k) \) and \( m \) a positive integer greater than \( |Y_i| \) where \( Y := \cup_{i \in I} Y_i \).

Proposition 2.2. There is a subset \( \Sigma \) of \( E(k') \) where \( k' \) is a finite extension of \( k \) which satisfies the following properties.

1. \( |\Sigma| = m, \quad \Sigma \cap Y = \varnothing. \)
2. \( C_{\ell_i}((Y_i), \Sigma) \) is MDS for all \( i \in I \).

Proof. For a positive integer \( t \) less than \( m \), let \( \mathcal{J}_t \) be the collection of subsets of \( \{1, \ldots, m\} \) with cardinality \( t \) and we associate the projection \( \pi_J \) with \( J \in \mathcal{I}_t \) by
\[
\pi_J : E^m \to E^t, \quad \pi_J(x_1, \ldots, x_m) = (x_j)_{j \in J}.
\]
Put \( d_i = |Y_i| \) and we define an epimorphism \( \sigma_i : E^{d_i} \to E \) to be
\[
\sigma_i(x_1, \ldots, x_{d_i}) = \sum_{j=1}^{d_i} x_j - \sum_{y \in Y_i} y.
\]

Let \( \sigma_J \) be the composition \( \sigma_J := \sigma_i \cdot \pi_J \) for \( J \in \mathcal{J}_{d_i} \). We define the divisors \( Z, W \) and \( \Delta \) of \( E^m \) as follows:

1. \( W := \cup_{i=1}^m \pi_i^{-1}(Y_i), \quad \) where \( \pi_i \) is the projection to the \( i \)-th factor.
2. \( Z := \cup_{i \in I} \cup_{J \in \mathcal{J}_{d_i}} \sigma_J^{-1}(0). \)
3. \( \Delta := \{(x_1, \ldots, x_m) \in E^m \mid x_i = x_j \quad (\exists i \neq j)\}. \)

Take \( x = (x_1, \ldots, x_m) \in E(k')^m \setminus (Z \cup W \cup \Delta) \) and we define a subset \( \Sigma \) of \( E \) as \( \Sigma := \{x_1, \ldots, x_m\} \). Here note that such \( x \) exists if \( k' \) is sufficiently large. The condition (1) implies that \( x_i \notin Y \) for all \( i \) and \( \Sigma \cap Y = \varnothing. \) We find that \( |\Sigma| = m \) by (3). The condition (2) shows that \( (Y_i) - (\sum_{j \in J} x_j) \) is not principal for \( \forall J \in \mathcal{J}_{d_i} \) (\( \forall i \in I \)). Hence \( C_{\ell_i}((Y_i), \Sigma) \) is MDS for all \( i \in I \) as we have explained in the introduction.

The following theorem is clear from Lemma 2.1, Proposition 2.1 and Proposition 2.2.

Theorem 2.1. Let \( \{X_i\}_i \) be a finite family of subsets of \( E(k) \) which meet at a single point. Set \( X := \cup_i X_i \) and let \( m \) be an arbitrary integer greater than \( |X| \). Then there is a subset \( \Sigma \) of \( E(k') \setminus X \) where \( k' \) is a finite extension of \( k \) such that

1. \( |\Sigma| = m. \)
2. \( C_{\ell_i}^0((X), \Sigma^*) \) and \( C_{\ell_i}^0((X_i), \Sigma^*) \) (\( \forall i \)) are MDS.
(3) $\mathcal{L}_0((\cup_i X_i))$ has a proper decomposition,
$$\mathcal{L}_0((X)) = \oplus_i \mathcal{L}_0((X_i)).$$

In order to describe the projector explicitly we impose a certain structure of $\{X_i\}_i$, which will be discussed in the following sections.

3. The kernel of an isogeny

Let $q$ be a power of a prime $p$ and set $k = \mathbb{F}_q$ and $k_m = \mathbb{F}_{q^m}$. Let $E$ be an elliptic curve defined over $k$. Take a prime $l \neq p$ and we consider a representation $\rho_l : \text{End}_k(E) \to \text{End} T_l(E)$, where $T_l(E)$ is the $l$-adic Tate module. We recall facts which will be used later.

Fact 3.1. \cite{4}

(1) $\deg f = \det \rho_l(f), \quad f \in \text{End}_k(E)$.

(2) Let $F$ be the $q$-th power endomorphism of $E$ and $\{\alpha, \beta\}$ eigenvalues of $\rho_l(F)$. Then they are algebraic integers with modulus $\sqrt{q}$ and are mutually complex conjugate.

(3) $|E(k_m)| = (1 - \alpha^m)(1 - \beta^m) = |1 - \alpha^m|^2$.

For positive integers $m$ and $n$ we define an endomorphism $\tau_{mn/m}$ of $E$ by
$$\tau_{mn/m} = \frac{\sum_{i=0}^{n-1} F^{im}}{1 - F^m} = \frac{1 - F^{mn}}{1 - F^m}.$$

Then
$$\tau_{mn/1} = \frac{1 - F^{mn}}{1 - F} = \frac{1 - F^{mn}}{1 - F} \frac{1 - F^m}{1 - F} \frac{1 - F^m}{1 - F} = \tau_{mn/m} \cdot \tau_{m/1}.$$

Let $G_m$ be the kernel of $\tau_{m/1}$. Since the differential of $\tau_{m/1}$ is equal to 1, $\tau_{m/1}$ is separable and $G_m$ is a reduced subgroup of $E$. In particular $\deg(\tau_{m/1}) = |G_m|$

Lemma 3.1.

(1) If $m|n$, $G_m \subseteq G_n$.

(2) The order of $G_m$ is $|\langle \alpha \rangle_m|^2$.

(3) $G_m$ is contained in $E(k_m)$ and
$$0 \to G_m \to E(k_m) \xrightarrow{\tau_{m/1}} E(k) \to 0.$$ 

Proof. (1) follows from the equation (3).

(2) Since $|G_m| = \deg \tau_{m/1}$ Fact 3.1 (1) and (2) show
$$|G_m| = \det \rho_l(\tau_{m/1}) = \left(\sum_{i=0}^{m-1} \alpha^i\right) \left(\sum_{i=0}^{m-1} \beta^i\right) = |\langle \alpha \rangle_m|^2.$$

(3) Take $x \in G_m$ and
$$(F^m - 1)(x) = (F - 1)\tau_{m/1}(x) = 0.$$
Thus $F^m(x) = x$, which shows $G_m \subset E(k_m)$. On the other for $y \in E(k_m)$,

$$(F - 1)\tau_{m/1}(y) = (F^m - 1)(y) = 0,$$

and $\tau_{m/1}(y) \in E(k)$. Thus we have an exact sequence

$$0 \to G_m \to E(k_m) \xrightarrow{\tau_{m/1}} E(k).$$

Since by Fact 3.1(3), $|E(k_m)| = |1 - \alpha^m|^2 = |(\alpha)_m|^2|1 - \alpha|^2 = |G_m| \cdot |E(k)|$ and $\tau_{m/1}$ is surjective. □

Remark 3.1. From the proof, we see that the degree of $\tau_{m/1}$ is $|\alpha_m|^2$, which is prime to $p$ by Fact 3.1(2).

Lemma 3.2. Suppose that $\gcd(m, n) = 1$. Then

$$G_m \cap G_n = 0.$$

Proof. Since $m$ and $n$ are coprime $E(k_m) \cap E(k_n) = E(k)$ and $G_m \cap G_n \subset E(k)$ by Lemma 3.1(3). Take $x \in G_m \cap G_n$. Because $F(x) = x$,

$$0 = \tau_{m/1}(x) = \sum_{i=0}^{m-1} F^i(x) = mx,$$

and similarly $nx = 0$. Since $\gcd(m, n) = 1$, $x = 0$. □

Proposition 3.1. Let $m$ and $n$ be positive coprime integers. Then

$$\ker(\tau_{m/1}\tau_{n/1}) = G_m + G_n.$$

Remark 3.2. In fact by Lemma 3.2 RHS is a direct sum.

Proof. Since $\tau_{m/1}$ and $\tau_{n/1}$ commute,

$$G_m + G_n \subset \ker(\tau_{m/1}\tau_{n/1}).$$

We compare the orders of both sides. By Lemma 3.2, $|G_m + G_n| = |G_m| \cdot |G_n|$ and

$$|G_m + G_n| = \deg(\tau_{m/1})\deg(\tau_{n/1}) = \deg(\tau_{m/1}\tau_{n/1}) = |\ker(\tau_{m/1}\tau_{n/1})|,$$

which implies the claim. □

4. A construction of a code

We fix a positive square free integer $N$ and consider the base extension of $E$ to $\Spec k_N$, which will be denoted by the same letter. We describe the set of positive divisors of $N$ by $D(N)$. For $m \in D(N)$ we set

$$X_m := \cup_{r \in P(m)} G_r, \quad D_m := (X_m).$$

Lemma 3.1 implies that $X_m$ is contained in $G_m$ and that $D_m$ is defined over $k_m$. The following proposition is clear from Lemma 3.1 and Lemma 3.2.
Proposition 4.1.
\[ \deg(D_m) - 1 = \sum_{r \in P(m)} \{\deg(G_r) - 1\} = \sum_{r \in P(m)} \{|(\alpha)_r|^2 - 1\}. \]

Definition 4.1. For \( m \in \mathcal{D}(N) \) we define an endomorphism \( \pi_m \) of \( E \) to be
\[ \pi_m = \prod_{r \in P(m)} \tau_r/1. \]

The degree of \( \pi_m \) is \( \prod_{r \in P(m)} \deg(\tau_r/1) \), which is prime to \( p \) (cf. Remark 3.1). If \( m \) and \( n \) are coprime, \( \pi_m \cdot \pi_n = \pi_{mn} = \pi_n \cdot \pi_m \).

Proposition 4.2. Let \( m, n \in \mathcal{D}(N) \) be coprime.
1. \[ \text{Ker}(\pi_m) = \bigoplus_{r \in P(m)} G_r. \]
2. \[ 0 \to \text{Ker}(\pi_m) \to \text{Ker}(\pi_{mn}) \xrightarrow{\pi_m/1} \text{Ker}(\pi_n) \to 0. \]
3. \[ 0 \to \text{Ker}(\pi_m) \to E(k_{mn}) \xrightarrow{\pi_m/1} E(k_n) \to 0. \]
4. \[ X_m \subset \text{Ker}(\pi_m). \]
5. \[ \pi_m(X_{mn}) = X_n. \]

Proof. (1) and (2) follow from Proposition 3.1. Using Lemma 3.1(3) successively one obtain (3). (4) and (5) are the consequences of (1) and (2).

From Proposition 2.1 and Lemma 3.2, we obtain the following theorem.

Theorem 4.1.
\[ L_0(D_N) = \bigoplus_{r \in P(N)} L_0(D_r). \]

Lemma 4.1. If \( |E(k)| \geq 2 \),
\[ |E(k_N) \setminus X_N| > \deg(D_N)(= |X_N|). \]

Remark 4.1. Fact 3.1(2) and (3) imply that the assumption is satisfied if \( |k| \geq 5 \).

Proof. By Proposition 4.2 we see that
\[ X_N \subset G_N := \tau_{N/1}^{-1}(0), \quad E(k_N) \setminus G_N \subset E(k_N) \setminus X_N. \]
On the other hand since by Lemma 3.1(3), \( E(k_N) \setminus G_N = (\tau_{N/1})^{-1}(E(k) \setminus 0) \) and the assumption yields
\[ |E(k_N) \setminus G_N| \geq |G_N|. \]
and the claim is clear.
Therefore there is a subset $\Sigma$ of $E(k_N) \setminus \Spt(D_N)$ such that $|\Sigma| > \deg(D_N)$ (e.g. $\Sigma := E(k_N) \setminus X_N$). Hence by Lemma 2.1, $C_0^I(D_N, \Sigma^*)$ is NMDS and the decomposition of Theorem 4.1 is proper.

**Theorem 4.2.** Let $m$ be an arbitrary integer greater than $\deg(D_N)$. Then there is a subset $\Sigma$ of $E(k_N') \setminus \Spt(D_N)$ where $k_N'$ is a finite extension of $k_N$ such that

1. $|\Sigma| = m$.
2. $C_0^I(D_N, \Sigma^*)$ is an MDS code and the decomposition of Theorem 4.1 is proper.

**Proof.** The statement is clear from Theorem 2.1 and Lemma 3.2.

Let $m, n \in D(N)$ be coprime. Since $D_m \leq D_{mn}$, $H^0(E, \mathcal{O}(D_m))$ is a subspace of $H^0(E, \mathcal{O}(D_{mn}))$ and let $i$ be the inclusion. We denote the composition of $H^0(E, \mathcal{O}(D_m)) \xrightarrow{i} H^0(E, \mathcal{O}(D_{mn})) \xrightarrow{(\pi_n)_*} H^0(E, \mathcal{O}(D_m))$, by $p_{mn/m}$. Here the latter map is obtained by Proposition 4.2(5).

**Proposition 4.3.**

1. If $f \in H^0(E, \mathcal{O}(D_n))$, $(\pi_n)_*(f)$ is a constant.
2. $p_{mn/m}$ is an isomorphism so that $p_{mn/m}(1) = \deg(\pi_n) \neq 0$.

**Proof.** (1) By Proposition 4.2(4) $\pi_n(X_n) = 0$ and $(\pi_n)_*(f) \in H^0(E, \mathcal{O}(0)) = k_N$.

(2) It is sufficient to show that $p_{mn/m}$ is injective. For a rational function $f$ on $E$ let $\mathcal{P}(f)$ describe the set of poles. By definition

$$p_{mn/m}(f)(y) = \sum_{z \in \pi_n^{-1}(y)} f(z) = \sum_{\gamma \in \ker(\pi_n)} f(x + \gamma),$$

where $\pi_n(x) = y$. In particular $p_{mn/m}(1) = \deg(\pi_n)$. Suppose $f \in H^0(E, \mathcal{O}(D_m))$ satisfies that $p_{mn/m}(f) = 0$. Then

$$f(x) = - \sum_{\gamma \in \ker(\pi_n)} f(x + \gamma).$$

Since, by Proposition 4.2(1), the support $\Spt(\mathcal{P}(f))$ is contained in $\ker(\pi_m)$, $\Spt(\mathcal{P}(f)) \subset \ker(\pi_m) + \gamma$. Thus (5) shows

$$\Spt(\mathcal{P}(f)) \subset \bigcup_{\gamma \neq 0 \in \ker(\pi_n)} \{ \ker(\pi_m) \cap \{ \ker(\pi_m) + \gamma \} \}.$$

But $\ker(\pi_m) \cap \{ \ker(\pi_m) + \gamma \} = \phi$ for $\gamma \neq 0 \in \ker(\pi_n)$ because $\ker(\pi_m) \cap \ker(\pi_n) = 0$ by Lemma 3.2 (Here note that $\ker(\pi_m) \subset G_m$ by Lemma 3.1(1) and Proposition 4.2(1)). Thus $f$ should be a constant and

$$p_{mn/m}(f) = \deg(\pi_n)f.$$

Since $\deg(\pi_m)$ is prime to $p$ as we have mentioned in Remark 3.1 so is $\deg(\pi_m)$ and we obtain the claim.

□
For $r \in P(N)$ we define
\[ \phi_{N/r} : H^0(E, \mathcal{O}(D_N)) \to H^0(E, \mathcal{O}(D_r)), \quad \phi_{N/r} := (p_{N/r})^{-1} \cdot (\pi_{N/r})^* . \]

Then by definition,
\[ (5) \quad \phi_{N/r}(h) = h, \quad h \in H^0(E, \mathcal{O}(D_r)), \]
and if $g \in H^0(E, \mathcal{O}(D_{r'}))$ ($r' \neq r \in P(N)$), $\phi_{N/r}(g)$ is a constant by Proposition 4.3.

Set $\phi^0_{N/r}(f) := \phi_{N/r}(f) - \phi_{N/r}(f)(P), \quad f \in H^0(E, \mathcal{O}(D_N))$.

Theorem 4.3. $\phi^0_{N/r}$ is a linear map from $H^0(E, \mathcal{O}(D_N))$ to $\mathcal{L}_0(D_r)$ satisfying the following properties.

1. $\phi^0_{N/r}(h) = h, \quad h \in \mathcal{L}_0(D_r)$.
2. If $r' \neq r$,
   \[ \phi^0_{N/r}(h) = 0, \quad h \in \mathcal{L}(D_{r'}). \]
3. For $f \in \mathcal{L}_0(D_N)$,
   \[ f = \sum_{r \in P(N)} \phi^0_{N/r}(f) . \]

Proof. (1) and (2) are clear from the definition. By Theorem 4.1 we may describe $f = \sum_{s \in P(N)} f_s, \quad f_s \in \mathcal{L}_0(D_s)$. Use (1) and (2), and
\[ \phi^0_{N/r}(f) = \sum_{s \in P(N)} \phi^0_{N/r}(f_s) = f_r, \]
which shows (3).

Now Theorem 1.1 and Theorem 1.2 follow from Proposition 4.1, Theorem 4.1, Theorem 4.2 and Theorem 4.3.

5. Error correcting pairs

Let $k$ be a finite field of characteristic $p$. For a finite set $\Sigma = \{s_1, \ldots, s_n\}$, we identify $k^\Sigma$ with $k^n$ as the introduction. The bilinear form $(\cdot, \cdot)$ on $k^n$ is defined by $(x, y) = \sum_i x_i y_i$. If $V$ is a linear subspace of $k^n$ let $V^\perp$ be the orthogonal complement; $V^\perp = \{x \in k^\Sigma | (x, v) = 0, \forall v \in V\}$. For $x, y \in k^n$ the star multiplication $x \ast y \in k^\Sigma$ is defined by the coordinate-wise multiplication, that is $(x \ast y)_i = x_i y_i$. For two subset $A$ and $B$ of $k^n$ we denote the set $\{a \ast b | a \in A, b \in B\}$ by $A \ast B$. Now let $e : C \to \mathbb{F}^n$ be a code.

Definition 5.1. A $t$-error correcting pair $(A, B)$ for $C$ is defined to be a pair of linear subspace $A$ and $B$ of $k^n$ satisfying the following conditions:

1. $A \ast B \subseteq e(C)^\perp$.
2. $\dim(A) > t$. 


effective algorithm which corrects 

\[
\text{Fact 5.1. (2) \text{Theorem 2.14}} \] 
If \((A, B)\) is a t-error correcting pair for \(C\), there is an effective algorithm which corrects \(t\)-errors with complexity \(O(n^3)\).

For the actual algorithm see [2] Algorithm 2.13. We will apply the Fact 4.1 to our code. Let \(N\) be a positive square free integer and \(m \in D(N)\). Let \(\Sigma\) be a finite subset of \(E\) disjoint from \(\text{Spt}(D_N)\) with \(|\Sigma| > \deg(D_N)\). We choose an arbitrary point \(P\) of \(\Sigma\) and set \(\Sigma^* : = \Sigma \setminus P\) as before. Embed \(L_0(D_m)\) into \(L(D_m)\) and we will find \(d^*\)-error correcting pair for \(C_L(D_m, \Sigma^*)\). Here

\[
d^* : = \left\lfloor \frac{1}{2}(\Sigma^* - \deg(D_m)) \right\rfloor - 1,
\]
where \(\lfloor x \rfloor\) is the maximal integer less than or equal to \(x\). Since \(d(C_L(D_m, \Sigma^*)) \geq |\Sigma^*| - \deg(D_m)\), \(d^*\) is the maximal weight of errors which may be corrected.

In general let \(\Sigma\) be a subset of \(E(k)\). Let \(D\) be an effective divisor defined over \(k\) whose support is disjoint from \(\Sigma\). We denote the image of

\[
e : H^0(E, \mathcal{O}(D)) \to k^E, \quad e(f)(x) = f(x),
\]
and

\[
r : H^0(E, \Omega^1((\Sigma) - D)) \to k^E, \quad r(\omega)(x) = \text{Res}_x(\omega),
\]
by \(C_L(D, \Sigma)\) and \(C_{\Omega^1}((\Sigma) - D, \Sigma)\), respectively. Here \(\text{Res}_x(\omega)\) is the residue of \(\omega\) at \(x\). Since the canonical sheaf \(\Omega\) is trivial, if we fix an invariant differential of \(E\), \(C_{\Omega^1}((\Sigma) - D, \Sigma)\) is identified with \(C_L((\Sigma) - D, \Sigma)\). Assume that \(\deg(D) < |\Sigma|\). Then the above maps are injective and the images are mutually orthogonal complement since the sum of all residues of a rational 1-form is zero.

\textbf{Proposition 5.1.} Suppose that \(d^*\) is positive. Then the pair of \(C_L((d^* + 1)(P), \Sigma^*)\) and \(C_{\Omega^1}((\Sigma^*) - D_m - (d^* + 1)(P), \Sigma^*)\) is a \(d^*\)-error correcting pair for \(C_L(D_m, \Sigma^*)\).

\textbf{Proof.} Note that the assumption implies that the evaluation maps, \(L(D_m) \xrightarrow{\psi^*} k^E\), \(L((d^* + 1)P) \xrightarrow{\psi^*} k^E\) and \(L(D_m + (d^* + 1)P) \xrightarrow{\psi^*} k^E\) are injective. Set

\[
A : = C_L((d^* + 1)(P), \Sigma^*), \quad B : = C_{\Omega^1}((\Sigma^*) - D_m - (d^* + 1)(P), \Sigma^*),
\]
and

\[
C : = C_L(D_m, \Sigma^*),
\]
and we will check whether the conditions of Definition 5.1 are satisfied. The star multiplication \(A \ast B\) is contained in \(C_{\Omega^1}((\Sigma^*) - D_m, \Sigma^*)\), which is the orthogonal complement of \(C\). Hence (1) has been checked. Since \(\dim(A) = d^* + 1\), (2) is clear. For (3) note that

\[
d(A) \geq |\Sigma^*| - (d^* + 1), \quad d(C) \geq |\Sigma^*| - \deg(D_m),
\]
and

\[
d(A) + d(C) - |\Sigma^*| \geq |\Sigma^*| - \deg(D_m) - (d^* + 1) \geq d^* + 1 > 0.
\]
Finally we check (4). Observe that
\[ B^\perp = C_L(D_m + (d^* + 1)(P), \Sigma^*), \]
and
\[ d(B^\perp) \geq |\Sigma^*| - \deg(D_m) - (d^* + 1) \geq \frac{1}{2}(|\Sigma^*| - \deg(D_m)) \geq d^* + 1. \]

\[ \square \]

**Corollary 5.1.** The pair of \( C_L((d^* + 1)(P), \Sigma^*) \) and \( C_\Omega((\Sigma^* - D_m - (d^* + 1)(P), \Sigma^*) \)

is a \( d^* \)-error correcting pair for \( e^*(\mathcal{L}_0(D_m)) \).

**Remark 5.1.** The minimal distance of \( C_L^0(D_m, \Sigma^*) \) is greater than or equal to \( |\Sigma| - \deg(D_m) \) and
\[ d^* = \left\lfloor \frac{1}{2}(|\Sigma| - \deg(D_m)) \right\rfloor - 1, \]
if \( |\Sigma| - \deg(D_m) \) is odd.

Thus we have an effective decoding algorithm of \( C_L^0(D_m, \Sigma^*) \) with complexity \( O(|\Sigma|^3) \) that corrects at most \( d^* \)-errors.

6. **Examples**

Suppose that \( p \geq 5 \) and let \( q = p^e \). Let \( E \) be an elliptic curve over \( k = \mathbb{F}_q \) which is the base extension of a supersingular elliptic curve defined over \( \mathbb{F}_p \). The eigenvalues of the \( q \)-th power Frobenius \( F \) are \( \{\alpha, \beta\} = \{\sqrt{-p}^e, -\sqrt{-p}^e\} \) and the characteristic polynomial of \( \rho_l(F) \) is \( x^2 + q \) if \( e \) is odd and is \( (x + \sqrt{q})^2 \) if \( e = 2f \) where \( f \) is odd.

**Fact 6.1.** \([5]\) Let \( n \) be a positive odd integer.

1. Suppose that \( p \equiv 1 \pmod{4} \) and that \( e \) is odd. Then
   \[ E(k_n) \simeq \mathbb{Z}/(1+q^n)\mathbb{Z}. \]

2. Suppose that \( e = 2f \) where \( f \) is odd. Then
   \[ E(k_n) \simeq \mathbb{Z}/(1+\sqrt{q}^n)\mathbb{Z} \oplus \mathbb{Z}/(1+\sqrt{q}^n)\mathbb{Z}. \]

Let \( m \) be a positive odd integer. Combine **Lemma 3.1(2)**, **Proposition 4.1** and **Fact 6.1** and we obtain the following proposition.

**Proposition 6.1.** Let \( N \) be a positive odd square free integer.

1. Suppose that \( p \equiv 1 \pmod{4} \) and that \( e \) is odd. Then
   \[ \deg(D_r) = (-q)_r, \quad \forall r \in P(N), \]
   and
   \[ |X_N| = \deg(D_N) = 1 + \sum_{r \in P(N)} \{-q)_r - 1\}. \]

2. Suppose that \( e = 2f \) where \( f \) is odd. Then
   \[ \deg(D_r) = (\sqrt{q})^2_r, \quad \forall r \in P(N), \]
   and
   \[ |X_N| = \deg(D_N) = 1 + \sum_{r \in P(N)} \{(\sqrt{q})^2_r - 1\}. \]
We fix an integer $m$ greater than $|X_N|$ and let $Z$, $W$ and $\Delta$ be divisors of $E^m$ appeared in the proof of \textbf{Proposition 2.2}.

\textbf{Proposition 6.2}. Let $n$ and $N$ be a positive odd integers satisfying $n > N$ and we assume that $N$ is square free.

(1) Suppose that $p \equiv 1 \pmod{4}$ and that $e$ is odd. Then

$$|E(k_n)^m \setminus (Z \cup W \cup \Delta)| \geq (1+q^n)^m - 1 + q^n - m + \frac{m}{2} - \sum_{r \in P(N)} \{m((-q)_r-1) + \left(\frac{m}{(-q)_r}\right)\}. $$

(2) Suppose that $e = 2f$ where $f$ is odd. Then

$$|E(k_n)^m \setminus (Z \cup W \cup \Delta)| \geq (1+\sqrt{q^n})^2(1+\sqrt{q^n})^2 - m - \sum_{r \in P(N)} \{m((\sqrt{q})^2 - 1) + \left(\frac{m}{(\sqrt{q})^2}\right)\}. $$

\textbf{Proof}. (1) We follow the notation of the proof of \textbf{Proposition 2.2}. By definition

$$|W \cap E(k_n)^m| \leq \sum_{i=1}^{m} |\pi_i^{-1}(X_N) \cap E(k_n)^m| \leq m|X_N| \cdot |E(k_n)|^{m-1},$$

and

$$|W \cap E(k_n)^m| \leq m(1 + \sum_{r \in P(N)} \{(q^n)_r - 1\})(1 + q^n)^{m-1},$$

by \textbf{Fact 6.1} and \textbf{Proposition 6.1}. A simple observation shows

$$|\Delta \cap E(k_n)^m| \leq \left(\frac{m}{2}\right)|E(k_n)|^{m-1} = \left(\frac{m}{2}\right)(1 + q^n)^{m-1}.$$ 

Let $r \in P(N)$ and $J \in J_{[X_r]}$. Since $X_r$ is a subset of $E(k_n)$, $\sigma_J$ is an affine surjective map from $E(k_n)^m$ to $E(k_n)$ that is the translation of an surjective group homomorphism by $-\sum_{x \in X_r} x$. Hence

$$|\sigma_J^{-1}(0)| = |E(k_n)|^{m-1} = (1 + q^n)^{m-1}.$$ 

Since $|X_r| = (-q)_r$ by \textbf{Proposition 6.1}(1),

$$|Z \cap E(k_n)^m| \leq (1 + q^n)^{m-1} \sum_{r \in P(N)} \left(\frac{m}{(-q)_r}\right).$$

Therefore

$$|(\Delta \cup Z \cup W) \cap E(k_n)^m| \leq (1 + q^n)^{m-1}\left(\frac{m}{2}\right) + m + \sum_{r \in P(N)} \{m((-q)_r - 1) + \left(\frac{m}{(-q)_r}\right)\},$$

and the claim is obtained. One can prove (2) by the similar way.

\begin{flushright}
$\square$
\end{flushright}

The proof of \textbf{Proposition 2.2} yields the following theorem.

\textbf{Theorem 6.1}. Let $N$ be a positive odd square free integer and $m$ an integer as below. If an integer $n$ greater than $N$ satisfies one of the following conditions, there is a subset $\Sigma$ of $E(k_n)$ disjoint from $\text{Spt}(D_N)$ with $|\Sigma| = m$ such that $C^0 = (D_N, \Sigma^r)$ is MDS and that the decomposition $L_0(D_N) = \oplus_{r \in P(N)} L_0(D_r)$ is proper.
(1) Suppose that $p \equiv 1 \pmod{4}$ and that $e$ is odd. Let $m$ be an integer greater than $1 + \sum_{r \in P(N)} \{(−q)_r - 1\}$. Then
\[ q^n > m + \binom{m}{2} + \sum_{r \in P(N)} \{m(−q)_r - 1\} + \left( \binom{m}{(−q)_r} \right) - 1. \]

(2) Suppose that $e = 2f$ where $f$ is odd. Let $m$ be an integer greater than $1 + \sum_{r \in P(N)} \{((\sqrt{q})^2 - 1)\}$. Then
\[ (1 + \sqrt{q})^n > m + \binom{m}{2} + \sum_{r \in P(N)} \{m((\sqrt{q})^2 - 1)\} + \left( \binom{m}{(\sqrt{q})^2} \right). \]

Acknowledgement: This research is partially supported by JSPS Grant in Aid No. 22540068.

REFERENCES

[1] J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes. North Holland, Amsterdam, New York, Oxford, 1977.
[2] R. Pellikaan, On decoding by error location and dependent sets of error positions. Discrete Math., 106/107:369–381, 1992.
[3] M. A. Shokrollahi, On the weight distribution of elliptic codes. Research Report, Institut für Informatik, Univ. Bonn, 1990.
[4] J. Silverman, The Arithmetic of Elliptic Curves. Springer GTM series, 106, 1986.
[5] H. J. Zhu, Group structures of elementary super singular abelian varieties over finite fields. J. Number Theory, 81:292–309, 2000.