A NEW CONSTRUCTION OF ALGEBRAIC GEOMETRY CODE USING TRACE FUNCTION

NUPUR PATANKER AND SANJAY KUMAR SINGH

Abstract. In this note, we give a construction of Algebraic-Geometry codes on algebraic function field $F/\mathbb{F}_q$ using places of $F$ (not necessarily of degree one) and trace functions from various extensions of $\mathbb{F}_q$. We compute a bound on the dimension of this code. We also determine a bound on the minimum distance of this code in terms of $B_r(F)$ (the number of places of degree $r$ in $F$), $1 \leq r < \infty$. This code is a generalization of the geometric Goppa code, with no restriction on the length of the code except the support condition on divisors defining the code. We obtained few quasi-cyclic codes over $\mathbb{F}_p$ as examples of these codes.

1. Introduction

A linear code is a $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$, the $n$-dimensional standard vector space over a finite field $\mathbb{F}_q$. Such codes are used for transmission of information. It was observed by Goppa in 1975 that we can use algebraic function fields over $\mathbb{F}_q$ to construct a class of linear codes by choosing a divisor and some rational places of algebraic function field over $\mathbb{F}_q$.

A very useful method of constructing codes over $\mathbb{F}_q$ is to use the trace mapping $Tr : \mathbb{F}_q^m \to \mathbb{F}_q$, if a code over $\mathbb{F}_q^m$ is given. The codes so obtained are called trace codes. Many interesting codes over $\mathbb{F}_q$ can be represented as trace codes. Trace code, its dimension and Hamming weight have been studied in [1], [3], [4], [5], [6], [7], [8], [11], etc. Generalized hamming weights of trace codes have been studied in [9] and [10]. In [8], Conny Voss obtained an estimate for the weights of code words of trace codes by using the Hasse-Weil bound for the number of rational places over $\mathbb{F}_q^m$. In this note, we give a construction of Algebraic-Geometry codes $C_{tr}$ on algebraic function field $F/\mathbb{F}_q$ using places of $F$ (not necessarily of degree one) and trace functions from various extensions of $\mathbb{F}_q$. This code is a generalization of the geometric Goppa code, with no restriction on the length of the code except the support condition on divisors defining the code. By using ideas from [8], we compute a bound on the dimension of this code. We also determine a bound on the minimum distance of this code in terms of $B_r(F)$ (the number of places of degree $r$ in $F$), $1 \leq r < \infty$.

A linear code $C$ of length $n = ml$ over $\mathbb{F}_q$ is called a quasi-cyclic code of index $l$ if for every $(c_0, \cdots , c_{n-1}) \in C$ we have $(c_{n-l}, \cdots , c_0, \cdots , c_{n-l-1}) \in C$. Quasi-cyclic codes have been studied for many years. The algebraic structure has been studied in [18], [19], [20], [21], [22], [23].

2010 Mathematics Subject Classification. 14H05 (94B27 94B05).
[21], etc. In [17], the authors have studied geometric realisation of quasi-cyclic codes. In this note, we construct few quasi-cyclic codes over $\mathbb{F}_p$, where $p$ is prime, as examples of $C_{tr}$.

This note is organized as follows. In section 2, we recall some results about Goppa codes, Extensions of Algebraic function fields and Trace codes. In section 3, we give the definition of code $C_{tr}$. In section 4, we determine an upper bound on the dimension of code $C_{tr}$. In section 5, we determine lower bound on the minimum distance of code $C_{tr}$ under various conditions. In section 6, we conclude the note listing examples of quasi-cyclic code over $\mathbb{F}_p$ derived from the code $C_{tr}$.

2. Preliminaries

2.1. Goppa code. ([11], Chapter II.2) Goppa’s construction of linear code is described as follows:

Let $F'/\mathbb{F}_q$ be an algebraic function field of genus $g$. Let $P_1, \ldots, P_n$ be pairwise distinct places of $F'/\mathbb{F}_q$ of degree 1. Let $D := P_1 + \cdots + P_n$ and $G$ be a divisor of $F'/\mathbb{F}_q$ such that $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. The geometric Goppa code $C_{L}(D, G)$ associated with $D$ and $G$ is defined by

\[ C_{L}(D, G) := \{(x(P_1), \cdots, x(P_n)) | x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n. \]

Then, $C_{L}(D, G)$ is an $[n, k, d]$ code with parameters $k = \dim(\mathcal{L}(G)) - \dim(\mathcal{L}(G - D))$ and $d \geq n - \deg(G)$.

2.2. Extensions of Algebraic Function Fields. Let $F/K$ denotes an algebraic function field of one variable with full constant field $K$. The field $K$ is assumed to be perfect.

**Definition 2.1.** ([11], Chapter III.1.1) An algebraic function field $F'/K'$ is called an algebraic extension of $F/K$ if $F' \supseteq F$ is an algebraic field extension and $K' \supseteq K$. The algebraic extension $F'/K'$ of $F/K$ is called a finite extension if $[F' : F] < \infty$.

**Definition 2.2.** ([11], Chapter III.1.3) A place $P' \in \mathbb{P}_F$ is said to be an extension of $P \in \mathbb{P}_F$ if $P \subseteq P'$.

**Definition 2.3.** ([11], Chapter III.2.4) Let $R$ be a subring of $F/K$. An element $z \in F$ is said to be integral over $R$ if $f(z) = 0$ for some monic polynomial $f(X) \in R[X]$, i.e. if there are $a_0, \cdots, a_n \in R$ such that

\[ z^n + a_{n-1}z^{n-1} + \cdots + a_1z + a_0 = 0. \]

The next theorem describes a method which can often be used to determine all extensions of a place $P \in \mathbb{P}_F$ in $F'$. For convenience we introduce some notation.

$\bar{F} := F_P$ is the residue class field of $P$. 

\[ \bar{a} := a(P) \in \bar{F} \text{ is the residue class of } a \in \mathcal{O}_P. \]

If \( \psi(T) = \sum c_i T^i \) is a polynomial with coefficients \( c_i \in \mathcal{O}_P \), we set
\[
\tilde{\psi}(T) := \sum c_i T^i \in F[T].
\]

**Theorem 2.5.** (Kummer) (\cite{[11]}, III.3.7) Suppose that \( F' = F(y) \) where \( y \) is integral over \( \mathcal{O}_P \), and consider the minimal polynomial \( \phi(T) \in \mathcal{O}_P[T] \) of \( y \) over \( F \). Let
\[
\bar{\phi}(T) = \prod_{i=1}^r \gamma_i(T)^{\epsilon_i}
\]
be the decomposition of \( \bar{\phi}(T) \) into irreducible factors over \( F \). Choose monic polynomials \( \phi_i(T) \in \mathcal{O}_{F'}[T] \) with
\[
\bar{\phi}_i(T) = \gamma_i(T) \text{ and } \deg \phi_i(T) = \deg \gamma_i(T).
\]

Then for \( 1 \leq i \leq r \), there are places \( P_i \in \mathbb{P}_{F'} \) satisfying
\[
P_i | P, \phi_i(y) \in P_i \text{ and } f(P_i|P) \geq \deg \gamma_i(T).
\]

Moreover \( P_i \neq P_j \), for \( i \neq j \).

Under additional assumptions one can prove more: Suppose that at least one of the following hypotheses is satisfied:
\[
\epsilon_i = 1 \text{ for } i = 1, \ldots, r, \text{ or } \{1, y, \ldots, y^{n-1}\} \text{ is an integral basis for } P.
\]

Then there exists, for \( 1 \leq i \leq r \), exactly one place \( P_i \in \mathbb{P}_{F'} \) with \( P_i | P \) and \( \phi_i(y) \in P_i \). The places \( P_1, \ldots, P_r \) are all places of \( F' \) lying over \( P \), and we have \( \epsilon_i = e(P_i|P) \). The residue class field \( F'_P = \mathcal{O}_P/P_i \) is isomorphic to \( F[T]/(\gamma_i(T)) \), hence \( f(P_i|P) = \deg \gamma_i(T) \).

The next theorem we need gives an estimate for the number of places of a fixed degree \( r \). Given a function field \( F/\mathbb{F}_q \) of genus \( g \), we define
\[
B_r := B_r(F) := \{ P \in \mathbb{P}_F ; \deg P = r \}.
\]

**Theorem 2.5.** (\cite{[11]}, V.2.10) The estimate
\[
|B_r| - \frac{q^r}{r} \leq \left( \frac{q}{q-1} + 2g \frac{q^{1/2}}{q^{1/2} - 1} \right) \frac{q^{r/2}}{r} - 1 < (2 + 7g) \frac{q^{r/2}}{r}
\]
holds for all \( r \geq 1 \).

2.3. (\cite{[11]}, VIII.1) **Trace codes.** Consider the field extension \( \mathbb{F}_{q^m} \mid \mathbb{F}_q \), let \( Tr : \mathbb{F}_{q^m} \to \mathbb{F}_q \) denote the trace mapping. For \( a = (a_1, \ldots, a_n) \in (\mathbb{F}_{q^m})^n \), we define \( Tr(a) := (Tr(a_1), \ldots, Tr(a_n)) \in \mathbb{F}_q^n \).

**Definition 2.6.** (\cite{[11]}, Def. VIII.1.1) Let \( C \subseteq (\mathbb{F}_{q^m})^n \) be a code over \( \mathbb{F}_{q^m} \). Then
\[
Tr(C) := \{ Tr(c) \mid c \in C \} \subseteq \mathbb{F}_q^n
\]
is called the trace code of \( C \).
A subcode of a code $C \subseteq (\mathbb{F}_{q^m})^n$ means an $\mathbb{F}_{q^m}$-subspace $U \subseteq C$. By $U^q$ we denote the set

$$U^q := \{(a_1^q, \ldots, a_n^q) \mid (a_1, \ldots, a_n) \in U\}.$$ 

A bound on the dimension of the trace code is given by the following proposition.

**Proposition 2.7.** ([11], Theorem VIII.1.4) Let $C$ be a code over $\mathbb{F}_{q^m}$ and $U \subseteq C$ be a subcode with the additional property $U^q \subseteq C$. Then

$$\dim \text{Tr}(C) \leq m.(\dim C - \dim U) + \dim U|_{\mathbb{F}_q}.$$ 

### 3. Definition of code

Let $F/\mathbb{F}_q$ be an algebraic function field. Choose a positive integer $n$. Choose $n$ arbitrary places $P_1, \ldots, P_n$ of $F$. Let $D := P_1 + \cdots + P_n$. Let $\beta_i := \text{deg}(P_i)$. Choose a divisor $G$ of $F$ with $\text{supp}(G) \cap \text{supp}(D) = \emptyset$. Let $\text{Tr}_i$ denote the trace map from $\mathbb{F}_{q^{\beta_i}}$ to $\mathbb{F}_q$.

Consider the map

$$\phi : \left\{ \begin{array}{ccc} \mathcal{L}(G) & \to & \mathbb{F}^n_q \\ x & \mapsto & (\text{Tr}_1(x(P_1)), \ldots, \text{Tr}_n(x(P_n))) \end{array} \right.$$ 

Define $C_{tr} := \phi(\mathcal{L}(G))$. Then, $C_{tr}$ is a linear code of length $n$ over $\mathbb{F}_q$.

**Remark 3.1.** There is no restriction on the length of the code $C_{tr}$ except its support doesn’t intersect with $D$.

### 4. Dimension of code $C_{tr}$

We have $C_{tr}$ is a vector space over $\mathbb{F}_q$. Hence,

$$\dim_{\mathbb{F}_q} C_{tr} = l(G) - \dim_{\mathbb{F}_q} K$$

where $K$ is the kernel of $\phi$. Note that $\mathcal{L}(G - D) \subseteq K$. Let

$$E := \{ f \in \mathcal{L}(G) \mid f = h^q - h \text{ for } h \in F \}.$$ 

For any $f \in E$ we have $\phi(f) = \phi(h^q - h) = (0, \ldots, 0)$. Therefore, the $\mathbb{F}_q$-vector space generated by $\mathcal{L}(G - D) \cup E$ denoted by $\langle \mathcal{L}(G - D) \cup E \rangle$ is contained in $K$ and

$$\dim_{\mathbb{F}_q} C_{tr} \leq l(G) - \dim_{\mathbb{F}_q} \langle \mathcal{L}(G - D) \cup E \rangle.$$ 

Now, for a divisor $G = \sum_{P \in \mathbb{F}_q} n_P P$ we define the divisor $[\frac{G}{q}] := \sum_{n_P > 0} [\frac{n_P}{q}] P + \sum_{n_P < 0} n_P P$, where $\lfloor t \rfloor$ denotes the greatest integer function. For $h \in \mathcal{L}([\frac{G}{q}])$, we have $h^q - h \in \mathcal{L}(G)$ and $\phi(h^q - h) = (0, \ldots, 0)$. Consider the map

$$\psi : \left\{ \begin{array}{ccc} \mathcal{L}([\frac{G}{q}]) & \to & E \\ h & \mapsto & h^q - h \end{array} \right.$$
The kernel of the map $\psi$ is $\mathbb{F}_q \cap \mathcal{L}([\frac{G}{q}])$. Also $\mathcal{L}(G-D) \cap E = \psi(\mathcal{L}(\lfloor \frac{G}{q} \rfloor - D))$.

From the above discussion, we have the following result regarding the dimension of $C$,

**Theorem 4.1.** $\dim C_{tr} \leq l(G) - l(G-D) - l(\lfloor \frac{G}{q} \rfloor) + \dim (\mathbb{F}_q \cap \mathcal{L}(\lfloor \frac{G}{q} \rfloor)) + l(\lfloor \frac{G}{q} \rfloor - D) - \dim (\mathbb{F}_q \cap \mathcal{L}(\lfloor \frac{G}{q} \rfloor - D))$.

5. **Minimum distance of code $C_{tr}$**

In this section we apply the techniques of [11], VIII.2 to compute bound on the minimum distance of $C_{tr}$. Suppose $q = p^m$ where $m > 0$. We first assume that for all $1 \leq i, j \leq n$, $\beta_i$ is coprime to $p$ and $p\beta_i > \beta_j$ i.e degrees of $P_i$ are not $p$ times multiples of each other.

Given $\mathcal{L}(G)$, there exists a unique effective divisor $A$ of smallest degree such that $(f)_{\infty} \subseteq A$ for all $0 \neq f \in \mathcal{L}(G)$. One can describe $A$ as follows: choose a basis $\{f_1, \cdots, f_k\}$ of $\mathcal{L}(G)$ then

$$v_P(A) = \max\{v_P((f_i)_{\infty}) | 1 \leq i \leq k\}$$

for all $P \in \mathbb{P}_F$. We associate with the divisor $A$ a second divisor $A^0$ defined by

$$A^0 := \sum_{P \in supp \ A} P.$$

**Definition 5.1.** An element $f \in F$ is called degenerate if $f = \gamma + \alpha(h^p - h)$ where $\gamma \in \mathbb{F}_q$, $h \in F$ and $\alpha \in \mathbb{F}_q^*$. Otherwise, $f$ is said to be non-degenerate. A $\mathbb{F}_q$-subspace $V$ of $F$ is said to non-degenerate if every element of $V$ is non-degenerate.

**Remark 5.2.** Assume that $\mathcal{L}(G)$ is non-degenerate.

For $f \in \mathcal{L}(G)$, consider the field extension $E_f = F(y)$ defined by $y^q - y = f$. Consider the polynomial $\pi(Y) = Y^q - Y - f$. Since, $f$ is non-degenerate by [2] Lemma 1.3, we have $\pi(Y)$ is irreducible over $F$. Thus, $E_f$ is a Galois extension of degree $q$. Also,

**Lemma 5.3.** $\mathbb{F}_q$ is constant field of $E_f$.

**Proof.** Let $L \supseteq \mathbb{F}_q$ be the constant field of $F$. By definition of constant field extension,

$$[FL : L(x)] = [F : \mathbb{F}_q(x)]$$

$$\Rightarrow [FL : F] = [L(x) : \mathbb{F}_q(x)] = [L : \mathbb{F}_q]$$

$$\Rightarrow [L : \mathbb{F}_q] = [FL : F] \mid [E_f : F] = q$$

$$\Rightarrow [L : \mathbb{F}_q] = p^d \text{ for some } d < m$$

So, by Galois correspondence, there exists a field extension $L'$ of $\mathbb{F}_q$ such that $[L' : \mathbb{F}_q] = p$. Thus, by Artin-Schurier extension, $L' = \mathbb{F}_q(\alpha)$ where $\alpha^p - \alpha = \gamma \in \mathbb{F}_q$. Since, $\alpha \notin F \Rightarrow [F(\alpha) : F] = p$. By Elementary Abelian $p$-Extension, $F(\alpha) = F(y_\mu)$ where $y_\mu^p - y_\mu = \mu f$. $\Rightarrow y_\mu$ and $\alpha$ are two generators of Artin extension. So, they are related
as \( y_\mu = \beta \alpha + (b^\mu - b) \) for \( \beta \in \mathbb{F}_p^* \) and \( b \in F \). This implies, \( \mu f = \beta \gamma + (h^\mu - h) \). This is a contradiction as \( f \) is assumed to be non-degenerate. \( \square \)

5.1. Case I: All \( P_i \) have same degree \( \beta \). The support of \( D \) consists of two disjoint subsets \( \{ P_1, \cdots, P_n \} = N \cup Z \) where

\[
N := \{ P_i \in \text{supp}(D) \mid \text{Tr}_i(f(P_i)) \neq 0 \}
\]

and

\[
Z := \{ P_i \in \text{supp}(D) \mid \text{Tr}_i(f(P_i)) = 0 \}.
\]

Hilbert’s Theorem 90 states that for \( \gamma \in \mathbb{F}_q^* \),

\[
\text{Tr}(\gamma) = 0 \iff \gamma = \alpha^q - \alpha \text{ for some } \alpha \in \mathbb{F}_q.
\]

We would like to determine how the places \( P_i \) decompose in the extension \( E_f/\mathbb{F}_q \).

Let \( P_i \in N \) and \( \gamma_i := f(P_i) \in \mathbb{F}_q^* \). The Artin-Scherier polynomial \( Y^q - Y - \gamma_i \) has no root in \( \mathbb{F}_q^* \). Each irreducible factor of \( Y^q - Y - \gamma_i \) in \( \mathbb{F}_q^* \) has degree \( p \). So, by Kummer’s theorem there are no places of degree \( \beta \) in \( E_f \) over \( P_i \) in \( N \).

Next we consider a place \( P_i \in Z \). Then \( f(P_i) \) can be written as \( f(P_i) =: \gamma_i = \beta_i^q - \beta_i \in \mathbb{F}_q \), hence the polynomial \( Y^q - Y - \gamma_i \) factors over \( \mathbb{F}_q \) into \( q \) distinct places of \( E_f \), all of degree \( \beta \).

The above considerations imply that

\[
B_\beta(E_f) = q|Z| + |\bar{S}| = q(n - |N|) + s.
\]

Therefore, \( w_f = |N| = n - \frac{B_\beta(E_f) - s}{q} \). Applying Theorem 2.5, we get

\[
w_f > n - (2 + 7q(E_f))\frac{q^{\beta/2 - 1}}{\beta} - \frac{q^{\beta - 1}}{\beta}.
\]

Theorem 5.4. If \( \mathcal{L}(G) \neq \emptyset \) and \( \mathcal{L}(G) \neq \mathbb{F}_q \), then the minimum distance \( d \) of \( C_{t_r} \) is bounded from below by

\[
d > n - 2\frac{q^{\beta/2 - 1}}{\beta} - \frac{q^{\beta - 1}}{\beta} - 7\frac{q^{\beta/2 - 1}}{\beta}[qg + \frac{(q - 1)}{2}(-2 + \deg A + \deg A^0)].
\]

5.2. Case II: Degrees of \( P_i \) are not same. Let \( \{ t_1, \cdots, t_r \} \) be the set of distinct \( \beta_i \)'s (where \( \beta_i = \deg P_i \) as defined before). For \( 1 \leq i \leq r \), let

\[
Z_i := \{ P_j \in \text{supp}(D) \mid \deg P_j = t_i \text{ and } \text{Tr}_j(f(P_j)) = 0 \text{ for some } j, 1 \leq j \leq n \}
\]

and

\[
N_i := \{ P_j \in \text{supp}(D) \mid \deg P_j = t_i \text{ and } \text{Tr}_j(f(P_j)) \neq 0 \text{ for some } j, 1 \leq j \leq n \}.
\]

Let

\[
Z := \bigcup_{i=1}^{r} Z_i \text{ and } N := \bigcup_{i=1}^{r} N_i.
\]
For \(1 \leq i \leq r\), let \(S_i := \{P \in \mathbb{P}_F \mid \deg P = t_i \text{ and } P \not\in \text{supp}(D)\}\) and \(\bar{S}_i := \{Q \in \mathbb{P}_{E_f} \mid \deg Q = t_i \text{ and } Q \cap F \in S_i\}\). Then as above, for \(1 \leq i \leq r\)
\[
B_{t_i}(E_f) = q|Z_i| + |\bar{S}_i|.
\]
Therefore,
\[
w_f > n - \sum_{i=1}^{r} \frac{q^{t_i-1}}{t_i} - (2 + 7g(E_f)) \sum_{i=1}^{r} \frac{q^{t_i/2}}{t_i}.
\]

**Theorem 5.5.** If \(\mathcal{L}(G) \neq 0\) and \(\mathcal{L}(G) \neq \mathbb{F}_q\), then the minimum distance \(d\) of \(C_{tr}\) is bounded from below by
\[
d > n - \sum_{i=1}^{r} \frac{q^{t_i-1}}{t_i} - 2 \sum_{i=1}^{r} \frac{q^{t_i/2}}{t_i} - 7 \sum_{i=1}^{r} \frac{q^{t_i/2}}{t_i}[qg + \frac{(q-1)}{2}(-2 + \deg A + \deg A^0)].
\]

Now we consider the case when degrees of \(P_i\) are \(p\) times multiple of each other.

Suppose \(t_{i,j}, 1 \leq i \leq r\) and \(1 \leq j \leq s_i - 1\) be the set of distinct \(\beta_i\)'s such that for \(1 \leq i \leq r\) and \(1 \leq j \leq s_i - 2\), \(t_{i,j} = pt_{i,j+1}\). For \(1 \leq i \leq r\) and \(1 \leq j \leq s_i - 1\), let
\[
Z_{i,j} := \{P_i \in \text{supp}(D) \mid \deg P_i = t_{i,j} \text{ and } Tr_t(f(P_i)) = 0\}
\]
and
\[
N_{i,j} := \{P_i \in \text{supp}(D) \mid \deg P_i = t_{j,i} \text{ and } Tr_t(f(P_i)) \neq 0\}.
\]
Let
\[
Z := \bigcup Z_{i,j} \text{ and } N := \bigcup N_{i,j}.
\]

Let \(P_i \in N\) then \(P_i \in N_{i,j}\) for some \(i, j\) such that \(\deg P_i = t_{i,j}\) and \(\gamma_i := f(P_i) \in \mathbb{F}_{q^{t_{i,j}}}\). The polynomial \(Y^q - Y - \gamma_i\) has no root in \(\mathbb{F}_{q^{t_{i,j}}}\). It decomposes into \(m\) places of degree \(pt_{i,j} = t_{i,j-1}\). Now for some \(Q_i \in Z\) with \(\deg Q_i = t_{i,j-1}\), by Kummer's theorem \(Q_i\) has \(q\) extensions all of degree \(t_{i,j-1}\).

Let \(S_{i,j} := \{P \in \mathbb{P}_F \mid \deg P = t_{i,j} \text{ and } P \not\in \text{supp}(D)\}\) and \(\bar{S}_{i,j} := \{Q \in \mathbb{P}_{E_f} \mid \deg Q = t_{i,j} \text{ and } Q \cap F \in S\}\).

The above considerations imply that
\[
B_{t_{i,j-1}}(E_f) = |\bar{S}_{i,j-1}| + q|Z_{i,j-1}| + m|N_{i,j}|.
\]
Applying Theorem 2.5 for \(B_{t_{i,j}}\) we get,
\[
|Z_{i,j}| < (2 + 7g(E_f)) \frac{q^{t_{i,j-1}}}{t_{i,j}} + \frac{q^{t_{i,j-1}}}{t_{i,j}}.
\]
Now, \(w_f = |N| = n - \sum_{i,j} Z_{i,j}\). Proceeding as above, we get
\[
w_f > n - \sum_{i=1}^{r} \sum_{j=1}^{s_i-1} \left[2 \frac{q^{t_{i,j}/2}}{t_{i,j}} + \frac{q^{t_{i,j-1}}}{t_{i,j}} - 7 \frac{q^{t_{i,j}/2}}{t_{i,j}}[qg + \frac{(q-1)}{2}(-2 + \deg A + \deg A^0)]\right].
\]
Theorem 5.6. If $L(G) \neq 0$ and $L(G) \neq F_q$, then the minimum distance $d$ of $C_{tr}$ is bounded from below by

$$d > n - \sum_{i=1}^{n} \sum_{j=1}^{s_i-1} 2^{q(t_{i,j}/2) - 1} - \sum_{j=1}^{s_i-1} 7^{q(t_{i,j}/2) - 1} [qq + (q - 1)(-2 + \text{deg } A + \text{deg } A^0)]].$$

6. Examples

6.1. Trace code. For $1 \leq i \leq n$, if $\beta_i = \text{deg } P_i = 1$, then we get the code $C_{tr}$ is the trace code of geometric goppa code.

6.2. Some examples of quasi-cyclic codes over $\mathbb{F}_p$. We let $q = p^r$ where $p$ is prime. For a positive integer $d$, it is well known that the number of monic irreducible polynomials of degree $d$ over $\mathbb{F}_q$, denoted by $N(d, q)$, is given by

$$(6.1) \quad N(d, q) = \frac{1}{d} \sum_{a | d} \mu(a)q^{d_a}.$$  

The trace of a polynomial $f(x)$ of degree $d$ over $\mathbb{F}_q$ is the coefficient of $x^{d-1}$ in $f$.

For $\gamma \in \mathbb{F}_q^*$, let $N_\gamma(d, q)$ denotes the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree $d$ and trace $\gamma$. Carlitz’s formula [12] for $N_\gamma(d, q)$ when $\gamma \neq 0$ is

$$N_\gamma(d, q) = \frac{1}{qd} \sum_{a | d, \ p \not| a} \mu(a)q^{d_a}.$$  

Lemma 6.1. ([13], Lemma 2.1) If $\gamma$ and $\delta$ are non-zero elements of $\mathbb{F}_q$ then $N_\gamma(d, q) = N_\delta(d, q)$.

Proposition 6.2. ([13], Corollary 2.8) Write $d = p^k b$ with $p \not| b$. Then

$$N_0(d, q) = \frac{1}{dq} \sum_{a | b} \mu(a)q^{d_a} - \epsilon \sum_{a | b} \mu(a)q^{d_a}$$

where $\epsilon = 1$ if $k > 0$ and $\epsilon = 0$ if $k = 0$.

Proposition 6.3. ([14], Theorem 9.5) Let $\mathbb{Z}_p$ be a subfield of two isomorphic finite fields $K_1$ and $K_2$. If $\sigma$ is a field isomorphism from $K_1$ onto $K_2$ that fixes the elements of $\mathbb{Z}_p$, then for $a_1 \in K_1$,

$$Tr_{K_1}(a_1) = Tr_{K_2}(\sigma(a_1)).$$

Fix a prime $p$ and positive integers $d$ and $m$ such that $(d, p) = 1$. Consider the finite field $\mathbb{F}_p$ where $p$ is a prime. Then from Lemma 6.1 and Proposition 6.2, we have for any $\gamma \in \mathbb{F}_p^*$ we have $N_0(d, p) = N_0(d, p) =: m$.

Let $Tr_d$ denotes the trace function

$$Tr : \mathbb{F}_{p^d} \to \mathbb{F}_p, a \mapsto a + a^p + \cdots a^{p^{d-1}}.$$
Choose \( \alpha \in \mathbb{F}_p \) such that \( d\alpha \equiv 1 \mod p \) or in other words \( Tr_d(\alpha) = 1 \) (such a \( \alpha \) always exist since \( (d, p) = 1 \)). Let \( A \) denotes the set of all monic irreducible polynomials of degree \( d \) over \( \mathbb{F}_p \). We know that automorphism group of rational function field \( \text{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p) = PGL(2, p) \) is the projective linear group over \( \mathbb{F}_p \) i.e any \( \phi \in \text{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p) \) is of the form

\[
\phi(x) = \frac{ax + b}{cx + d}
\]

where \( a, b, c, d \in \mathbb{F}_p \) such that \( ad - bc \neq 0 \).

Let \( \theta \in \text{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p) \) given by \( \theta(x) := x + \alpha \).

Since for any \( f(x) \in A \) i.e for monic irreducible polynomial \( f(x) \in \mathbb{F}_p[x] \) of degree \( d \), we have \( f(x + \alpha) \) is monic and irreducible of degree \( d \) i.e \( f(x + \alpha) \in A \) and conversely. Order the elements of \( A \) as

\[
\begin{align*}
& p_{0,1}, \ p_{0,2}, \ \cdots, \ p_{0,m} \\
& p_{1,1}, \ p_{1,2}, \ \cdots, \ p_{1,m} \\
& \vdots \quad \vdots \quad \vdots \quad \vdots \\
& p_{p-1,1} \ p_{p-1,2} \ \cdots, \ p_{p-1,m},
\end{align*}
\]

where for \( 1 \leq i \leq p \), the \( i \)-th row consists of elements of \( A \) with trace \(-i - 1 \in \mathbb{F}_p \) and for \( 0 \leq \gamma \leq p - 2 \), \( 1 \leq \beta \leq m \) \( p_{\gamma+1,\beta}(x) = \theta(p_{\gamma,\beta}(x)) \). Then the corresponding set of places of \( \mathbb{F}_p(x)/\mathbb{F}_p \) is

\[
\begin{align*}
& P_{0,1}, \ P_{0,2}, \ \cdots, \ P_{0,m} \\
& P_{1,1}, \ P_{1,2}, \ \cdots, \ P_{1,m} \\
& \vdots \quad \vdots \quad \vdots \quad \vdots \\
& P_{p-1,1} \ P_{p-1,2} \ \cdots, \ P_{p-1,m},
\end{align*}
\]

Choose a positive integer \( r \). Then the code \( C_{tr} \) with \( G := rP_\infty \) and \( D := \sum_{i=0}^{p-1} \sum_{j=1}^{m} P_{i,j} \) is

\[
C_{tr} = \{(Tr_{i,j}(z(P_{i,j})))_{0 \leq i \leq p-1, 1 \leq j \leq m} \mid z \in \mathcal{L}(rP_\infty)\}
\]

**Proposition 6.4.** The code \( C_{tr} \) as in equation (6.2) is quasi-cyclic code of length \( pm \) and index \( m \).

**Proof.** We have for \( \theta \) as defined before \( \theta(D) = D \) and \( \theta(\mathcal{L}(G)) = \mathcal{L}(G) \). Let \( \pi : \{0, 1, \cdots, p - 1\} \to \{0, 1, \cdots, p - 1\} \) be defined by \( \pi(j) = j + 1 \), for \( 0 \leq j \leq p - 2 \) and \( \pi(p - 1) = 0 \). We extend the action of \( \theta \) to \( C_{tr} \) as

\[
\theta((Tr_{i,j}(z(P_{i,j}))))_{0 \leq i \leq p-1, 1 \leq j \leq m}) := (Tr_{\pi(i),\pi(j)}(z(\theta(P_{i,j}))))_{0 \leq i \leq p-1, 1 \leq j \leq m}.
\]

We claim that \( Tr_{\pi(i),\pi(j)}(z(\theta(P_{i,j}))) = Tr_{i+1,j}(\theta^{-1}(z)(P_{i+1,j})) \).

We have the following diagram,

\[
\begin{array}{cccc}
\mathbb{F}_p[x] & \psi_2 & \mathbb{F}_p[x] \\
\downarrow \psi_1 & & \downarrow \psi_3 \\
F_{P_{i,j}} & \psi_4 & F_{P_{i+1,j}}
\end{array}
\]
where
\[
\psi_1(f(x) \mod p_{i,j}(x)) = f(x)(P_{i,j}),
\psi_3(f(x) \mod p_{i+1,j}(x)) = f(x)(P_{i+1,j}),
\psi_2(f(x) \mod p_{i,j}(x)) = f(x + \alpha) \mod p_{i+1,j}(x) = \theta(f(x)) \mod p_{i+1,j}(x)
\]
are field isomorphisms. Therefore, \(\psi_4\) is a field isomorphism between \(F_{P_{i,j}} \cong \mathbb{F}_{p^d}\) and \(F_{P_{i+1,j}} \cong \mathbb{F}_{p^d}\).

Now, \(Tr_{\tau(i,j)}(z(\theta(P_{i,j}))) = Tr_{i+1,j}(z(\theta(P_{i+1,j}))) = Tr_{i+1,j}(\psi_4(a(P_{i,j}))) = Tr_{i,j}(a(P_{i,j}))\), follows from Proposition 6.3.

Hence \(C_{tr}\) is quasi-cyclic of index \(m\). \(\square\)

**Example 6.5.** Consider the function field \(F_5(x) \setminus F_5\). There are 10 places of degree 2 of \(F_5(x) \setminus F_5\).

\[
\begin{align*}
P_1 &= P_{x^2+2}, & P_2 &= P_{x^2+3}, \\
P_3 &= P_{x^2+x+1}, & P_4 &= P_{x^2+x+2}, \\
P_5 &= P_{x^2+2x+3}, & P_6 &= P_{x^2+2x+4}, \\
P_7 &= P_{x^2+3x+3}, & P_8 &= P_{x^2+3x+4}, \\
P_9 &= P_{x^2+4x+1}, & P_{10} &= P_{x^2+4x+2}.
\end{align*}
\]

Let \(G := 2P_\infty\). Then the code \(C_{tr}\) so obtained has dimension \(k = 3\) and minimum distance \(d = 7\). The code has some good properties: It is a near MDS-code and also quasi-cyclic code of index 2.

### 7. Concluding Remarks

In this note, we have constructed generalised algebraic geometry codes. The code so obtained has no restriction on length. Also these codes contains few examples of quasi-cyclic codes.

### References

[1] Phong Le, Sunil Chetty. On the dimension of algebraic-geometric trace codes. Mathematics 4(2), 32.
[2] Arnaldo Garcia, Henning Stichtenoth. Elementary Abelian \(p\)-extensions of algebraic function fields. manuscripta mathematica, December 1991, Volume 72, Issue 1, pp 67-79.
[3] G. Lachaud, Artin-Schreier Curves, Exponential Sums and the Carlitz-Uchiyama Bound for Geometric Codes. J. of Number Theory 39 (1991), pp. 18-40.
[4] Carlos J. Moreno and Oscar Moreno, An improved Bombieri-Weil bound and applications to coding theory, Journal of Number Theory, Volume 42, Issue 1, September 1992, pp. 32-46.
[5] Gerard van der Geer and Marcel van der Vlugt, Trace codes and families of algebraic curves, Mathematische Zeitschrift volume 209, pp. 307-315 (1992).
[6] Marcel van der Vlugt, A new upper bound for the dimension of trace codes, Bull. London Math. Soc. 23 (1991), no. 4, pp. 395-400.
[7] Marcel van der Vlugt, On the dimension of trace codes, IEEE Trans. Inform. Theory 37 (1991), no. 1, pp. 196-199.
[8] Conny Voss, On the weights of trace codes, Coding theory and algebraic geometry (Luminy, 1991), 193-198, Lecture Notes in Math., 1518, Springer, Berlin, 1992.
[9] Henning Stichtenoth and Conny Voss, Generalized Hamming weights of trace codes, IEEE Trans. Inform. Theory 40 (1994), no. 2, pp. 554-558.
[10] Cem Güneri and Ferruh Özbudak, Improvements on Generalized Hamming Weights of Some Trace Codes, Designs, Codes and Cryptography volume 39, pp. 215-231 (2006).
[11] Henning Stichtenoth. Algebraic Function Fields and Codes. Springer-Verlag Berlin Heidelberg, 1993.
[12] L. Carlitz. A theorem of Dickson on irreducible polynomials. Proc. Amer. Math. Soc. 3 (1952)693700.
[13] Joseph L. Yucas. Irreducible polynomials over finite fields with prescribed trace/prescribed constant term. Finite Fields and Their Applications, Volume 12, Issue 2, April 2006, Pages 211-221.
[14] Chao Lu, Myoung An, and Richard Tolimieri. Mathematics of Multidimensional Fourier Transform Algorithms Second edition. Springer-Verlag Newyork In., 1993.
[15] Henning Stichtenoth. On automorphisms of geometric Goppa codes. Journal of Algebra, Volume 130, Issue 1, April 1990, Pages 113-121.
[16] Gintaras Skersys. On quasi-cyclic codes and traces of codes. Research papers from the XLV Conference of the Lithuanian Mathematical Society (Lithuanian). Liet. Mat. Rink. 44 (2004), Special Issue, 101-104.
[17] Cristina Martinez Ramirez and Alberto Besana. A Geometrical Realisation of Quasi-Cyclic Codes. In Book: Combinatorics, Probability and Control, November 19th 2019.
[18] San Ling, Patrick Solé. On the algebraic structure of quasi-cyclic codes. I. Finite fields. IEEE Trans. Inform. Theory 47 (2001), no. 7, 2751-2760.
[19] San Ling, Patrick Solé. On the algebraic structure of quasi-cyclic codes. II. Chain rings. Des. Codes Cryptogr. 30 (2003), no. 1, 113-130.
[20] San Ling, Patrick Solé. On the algebraic structure of quasi-cyclic codes. III. Generator theory. IEEE Trans. Inform. Theory 51 (2005), no. 7, 2692-2700.
[21] San Ling, Harald Niederreiter and Patrick Solé. On the Algebraic Structure of Quasi-cyclic Codes IV: Repeated Roots. Des. Codes Cryptogr. 38 (2006), no. 3, 337361.

Indian Institute of Science Education and Research, Bhopal

E-mail address: nupurp@iiserb.ac.in

Indian Institute of Science Education and Research, Bhopal

E-mail address: sanjayks@iiserb.ac.in