THE TRUE DIMENSION OF CERTAIN ALTERNANT CODES*

Yue Dianwu Feng Guangzeng
(Dept. of Telecom. Eng., Nanjing University of Posts & Telecommunications, Nanjing 210003)

Abstract By applying a result from geometric Goppa codes, due to H.Schtenoth, the true dimension of certain alternant codes is calculated. The results lead in many cases to an improvement of the usual lower bound for the dimension.

Key words Alternant code; Dimension; Algebraic function field; Geometric Goppa code

I. Introduction

Let $F_{q^m}$ be the finite field with $q$ a prime power and $m$ an integer. For a linear code $C$ defined over $F_{q^m}$, we denote by $C \mid F_q$ the restriction of $C$ to $F_q$.

Let $\mathcal{C} = (0/1, 0/2, \ldots, 0/n)$ with $0/i$ being distinct elements of $F_{q^m}$ and $y = (y_1, y_2, \ldots, y_n)$ with $y_i \in F_{q^m} - \{0\}$. For a positive integer $\gamma \leq n$, consider the matrix:

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{\gamma-1} & \alpha_2^{\gamma-1} & \cdots & \alpha_n^{\gamma-1} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}$$

Let $\zeta$ denote the code of length $n$ over $F_{q^m}$ with parity check matrix $H$. Define $A_\gamma(\alpha, y)$, then these codes are called alternant codes\cite{1}. Special cases of alternant codes are BCH codes and classical Goppa codes. For $k(A_\gamma)$ the dimension of $A_\gamma(\alpha, y)$, we have the inequality\cite{1}: $k(A_\gamma) \geq n - m \cdot \gamma$.

The aim of the present article is to improve the above-mentioned result. In section II, alternant codes are expressed as subfield subcodes of certain geometric Goppa codes. In section III, we first give a new lower bound to the dimension of alternant codes, and then derive the true dimension of certain alternant codes.

II. Alternant Codes and Subfield Subcodes of Geometric Goppa Codes

For a given alternant code $A_\gamma(\alpha, y)$, there exists exactly one polynomial $y(z)$ such that

$${\deg} y(z) < n, \quad y(\alpha_i) = 1/y_i, \quad i = 1, 2, \ldots, n$$

The polynomial $y(z)$ can be decomposed into distinct polynomial of the first degree $(z - \beta_u)$ over an algebraic closure of $F_{q^m}$ as $y(z) = \prod_{u=1}^{s} (z - \beta_u)^{m_u}$, where $m_u$ and $s$ are integers that satisfy the relation:

$$\sum_{u=1}^{s} m_u = {\deg} y(z), \quad m_u \geq 1, \quad s \geq 1$$

*Supported by the National Natural Science Foundation of China (No. 69872016)
The parameter $m_u$ can be rewritten as follows:

$$m_u = m_u^{(q)} \cdot q + m_u^{(0)}, \quad m_u^{(q)} \geq 0, \quad 0 \leq m_u^{(0)} \leq q - 1$$

Now we define the following two polynomials:

$$y_1(z) = \prod_{u=1}^{s} (z - \beta_u)^{m_u^{(q)}}, \quad y_2(z) = \prod_{u=1}^{s} (z - \beta_u)^{m_u^{(0)}}$$

Obviously, $y_1(z), y_2(z) \in \mathbb{F}_{q^m}[z]$. Let $b = \gamma - 1 - l$ with $l = \deg y(z)$. $b$ can be also expressed as:

$$b = b^{(q)} \cdot q + b^{(0)}, \quad b^{(q)} \geq 0, \quad 0 \leq b^{(0)} \leq q - 1$$

We will show that alternant codes can be represented as subfield subcodes of certain geometric Goppa codes. For that, we first briefly recall the notions of geometric Goppa codes (for a detailed introduction, see Refs.

Let $F/F_{q^m}$ be an algebraic function field of one variable whose constant field is exactly $F_{q^m}$. For a divisor $G$ of $F/F_{q^m}$, consider the space $L(G) = \{ f \in F \mid (f) \geq -G \}$ with denoting the principal divisor of $f$. From Ref.[2], $L(G)$ is a finite dimension vector space over $F_{q^m}$. Its dimension is denoted by $\dim G$. Assume that $P_1, P_2, \cdots, P_n$ are pairwise distinct places of $F/F_{q^m}$ of degree one that do not occur in the support of $G$. We write $D = P_1 + P_2 + \cdots + P_n$, and define the geometric Goppa code with respect to $G$ and $D$:

$$C_L(D, G) := \{(f(P_1), f(P_2), \cdots, f(P_n)) | f \in L(G)\} \subseteq (F_{q^m})^n$$

The dual code $C_L(D, G)^\perp$ can be also represented as $C_L(D, H)$ with a certain divisor $H$[5]. Usually, $C_L(D, G)^\perp$ is denoted by $C_O(D, G)$.

Let $F = F_{q^m}(z)$ be the rational function field over $F_{q^m}$ and $P_\infty$ be the pole of $z$[2]. For $i = 1, 2, \cdots, n$, denote by $P_i$ the zero of $(z - \alpha_i)$, and set $D_\alpha = P_1 + P_2 + \cdots + P_n$. Define $G_y = bP_\infty + \sum_{u=1}^{s} m_u Q_u$, where $Q_u$ is the zero of $(z - \beta_u)$ for $u = 1, 2, \cdots, s$.

**Theorem 1** $A_\gamma(\alpha, y) = C_{O}(D_\alpha, G_y) \mid F_q$.

**Proof** We consider the code $C_L(D_\alpha, G_y)$. Since $\dim G_y = l + b - 1 = \gamma$, the elements $z^iy(z)$ with $0 \leq i \leq \gamma - 1$ constitute a basis of $L(G_y)$. Hence the matrix $H$ (see Section I) is a generator matrix of $C_L(D_\alpha, G_y)$. So we can obtain easily the desired result. Q.E.D

### III. The Main Results

For a rational number $x$, $\lfloor x \rfloor$ denotes the maximal integer $\leq x$. For any divisor $G = \sum_{Q} m_Q Q$ with $m_Q$ being some integer (for the detailed definition of a divisor, see Ref.[2]), we define the divisor associated with $G$ as follows:

$$G' = \sum_{Q, m_Q \geq 0} \lfloor m_Q/g \rfloor Q + \sum_{Q, m_Q < 0} m_Q Q$$

**Theorem 2**[2] For a given geometric Goppa $C_{O}(D, G)$, we have

$$\dim (C_{O}(D, G) \mid F_q) \geq \begin{cases} n - 1 - m(\dim G - \dim G'), & G' \geq 0 \\ n - m(\dim G - \dim G'), & \text{otherwise} \end{cases}$$

Let $l_1 = \deg y_1(z)$. Applying Theorem 2 to alternant codes, we have the following corollary.