IMPROVEMENT ON PARAMETERS OF ALGEBRAIC-GEOMETRY CODES FROM HERMITIAN CURVES

SIMAN YANG

Abstract. Motivated by Xing’s method [7], we show that there exist \([n, k, d]\) linear Hermitian codes over \(\mathbb{F}_{q^2}\) with \(k + d \geq n - 3\) for all sufficiently large \(q\). This improves the asymptotic bounds given in [9, 10].

Keywords: Algebraic-geometry codes, asymptotic bounds, algebraic curves, algebraic function fields, Hermitian codes.

1. Introduction

We first review Goppa’s construction and properties of Algebraic-Geometry codes using the language of global function fields. A global function field \(F\) over a finite field \(\mathbb{F}_q\) is a function field having the following properties:

(i) \(F\) is an algebraic function field with constant field \(\mathbb{F}_q\).
(ii) \(\mathbb{F}_q\) is algebraically closed in \(F\).

A place of \(F\) is an equivalence class of valuations of \(F\). A place of \(F\) is rational if it has degree 1, i.e., its residue class field is \(\mathbb{F}_q\). A divisor of \(F\) is a formal sum \(\sum_P n_P P\) with \(n_P \in \mathbb{Z}\) and all but finitely many \(n_P = 0\). For a nonzero function \(f \in F\), the principal divisor \(\text{div}(f) = \sum_P \nu_P(f) P\), where \(\nu_P\) is the normalized discrete valuation corresponding to the place \(P\).

Denoted by \(N(F)\) the number of rational places of a function field \(F/\mathbb{F}_q\) and \(g(F)\) the genus of \(F/\mathbb{F}_q\). By the Hasse-Weil bound (cf. [4]) one has

\[ N(F) \leq q + 1 + 2g\sqrt{q}. \]  

(1.1)

Let \(F/\mathbb{F}_q\) be a global function field of genus \(g\) with \(n\) rational places, and \(G\) is a divisor of \(F\). The Riemann-Roch space associated to \(G\) consists of sections of \(G\), i.e., \(L(G) = \{ f \in F : \text{div}(f) + G \geq 0 \} \cup \{ 0 \}\) is a finite dimensional vector space over \(\mathbb{F}_q\). \(P_1, \ldots, P_n\) are distinct rational places of \(F\) with \(\{ P_1, \ldots, P_n \} \cap \text{supp}(G) = \emptyset\). An Algebraic-Geometry code is defined as the image of the \(\mathbb{F}_q\)-linear map from \(L(G)\) to \(\mathbb{F}_q^n : f \mapsto (f(P_1), \ldots, f(P_n))\). If \(g \leq \text{deg}(G) < n\), one gets linear \([n, k, d]\) code over \(\mathbb{F}_q\) with \(k = \dim(L(G)) \geq \text{deg}(G) + 1 - g\) (by the Riemann-Roch theorem), and \(d \geq n - \text{deg}(G)\) (because a nonzero section of \(G\) has at most \(\text{deg}(G)\) zeros), cf. [6]. Thus, \(k + d \geq n + 1 - g\).

The first author was partially supported by the program for Chang Jiang Scholars and Innovative Research Team in University.
Let $C$ be a linear code over an alphabet $\mathbb{F}_q$. Denoted by $n(C)$, $k(C)$, $d(C)$ the length, dimension, and minimum distance of $C$ respectively. We call the ratio $k(C)/n(C)$ the transmission rate and $d(C)/n(C)$ the error-detection rate of the code. It is a theoretical important task in coding theory to construct a sequence of codes with length goes to infinity together with asymptotic positive transmission rate and error-detection rate. Goppa’s construction of Algebraic-Geometry codes leads to the Tsfasman-Vladut-Zink bound [1] which is a breakthrough in coding theory as it beats the Gilbert-Varshamov bound in an open interval over a finite field of size $q_0^2$ with $q_0 \geq 7$. This motivates the construction of codes with parameters better than Goppa’s construction.

However, for about twenty years after Goppa’s construction, the refinement mainly concerned exhibiting suitable curves with “many” rational points (with respect to genus) and algorithmic improvement to the resulting codes. Recently, Xing [8] gave a new construction of nonlinear algebraic-geometry codes by exploiting the sections’ derivatives to find codes with better asymptotic parameters than Goppa’s. Elkies [2,3] estimated the size of the set of rational sections of bounded degree of the line bundle $L_D$ associated to a degree zero divisor $D$ on a curve $C$ to construct algebraic-geometry codes. His constructions also led to an improved asymptotic bound better than the Tsfasman-Vladut-Zink bound. Very recently, Stichtenoth, Niederreiter, Ozbudak and some others also constructed several nonlinear codes with better parameters than Goppa’s construction. In this paper we employ an idea of Xing [7] to yield linear codes from Hermitian curves with asymptotic parameters better than in the record (see [11], [9], [10]). Like all those codes mentioned above the codes we present are nonconstructive.

A maximal curve $F/\mathbb{F}_q$ of genus $g$ is a curve achieving the Hasse-Weil bound. Clearly, $q$ must be a square if there exists a maximal curve of positive genus over $\mathbb{F}_q$. Hermitian curves $F/\mathbb{F}_{q^2}$ are a class of important examples of maximal curves defined by an equation of the form

$$Y^q + Y = X^{q+1}. \quad (1.2)$$

It is known that $g(F) = (q^2 - q)/2$ and $N(F) = q^3 + 1$, among them, there are $q^3$ affine $\mathbb{F}_{q^2}$-rational points $P_1, \ldots, P_{q^3}$ and one infinite $\mathbb{F}_{q^2}$-rational point $P_\infty$ on this curve. It is obvious that Hermitian curves are maximal curves.

Yang and Kumar [11] determined the true minimum distance of one-point Hermitian codes as follows: For any integer $2g - 1 < t < q^3$, the one-point code $C_{L}(tP_\infty, D)$, where $D = P_1 + \ldots + P_{q^3}$, is a $[q^3, t - g + 1, d]$ linear code over $\mathbb{F}_{q^2}$ with $d = q^3 - t + c$ for some $0 \leq c < q$. This improved the Goppa’s estimate of minimum distance of Hermitian codes to $O(q)$. By employing a method of Xing [7], Xing and Chen [9], Xu[10] improved the Goppa’s estimate of minimum distance of Hermitian codes to $O(q^2)$ in some range respectively. The major effort here is expended on finding a specific divisor $G$ of a prescribed degree and satisfies $L(G - D') = \{0\}$ for all large subset $D' \subseteq \{P_1, \ldots, P_{q^3}\}$ of a prescribed degree. Our main result is as follows.
Theorem 1.1. There exist \([n, k, d]\) linear codes over \(\mathbb{F}_q^2\) with \(k + d \geq n - 3\) for all sufficiently large \(n = q^3\), where \(q\) is a prime power.

This improves the minimum distance of sufficiently large length Hermitian code very close to the genus of the relied curve than Goppa’s construction. We will use the following lemma in [7].

2. Codes from Hermitian Curves

Lemma 2.1. Let \(F\) be an algebraic curve with \(n\) rational points \(P_1, \ldots, P_n\). For fixed positive integers \(s > m\) define

\[
N_{s,m} = |\{ \sum_{P \in I} P + D : I \subseteq \{P_1, \ldots, P_n\}, |I| = m, D \geq 0, D = s - m \}|. \tag{2.1}
\]

Suppose \(N_{s,m} < h(F)\) (denoted by \(h(F)\) the class number of \(F\)). Then there exists a divisor \(G\) of degree \(s\) with \(\{P_1, \ldots, P_n\} \cap \text{supp}(G) = \emptyset\) and the AG code \(C_{L}(P_1, \ldots, P_n; G)\) is \([n, k, d]\) code with \(k = s - g + 1\) and \(d \geq n - m + 1\).

Obviously, the above construction can improve \(s - m + 1\) of Goppa’s estimate on minimum distance of Algebraic-geometry codes. We next search for such integers \(s\) and \(m\) satisfying Eq.(2.1) with large value \(s - m\) for a Hermitian curve \(F/\mathbb{F}_q^2\). To estimate \(N_{s,m}\) one needs to count the number of positive divisors of fixed degree. Thus it is natural to consider the zeta-function of \(F\) which is defined by

\[
Z_F(T) = \sum_{i=0}^{\infty} A_i T^i,
\]

where \(A_i\) is defined as the number of positive divisors of \(F\) of degree \(i\) for all integers \(i \geq 0\). It is well known that the zeta-function of a curve over \(\mathbb{F}_q^2\) is a rational function of the form

\[
Z_F(T) = \frac{L_F(T)}{(1 - T)(1 - q^2T)}
\]

We have the following upper bound of \(A_k\).

Proposition 2.2. For a maximal curve over \(\mathbb{F}_q^2\) with genus \(g\), it follows that

\[
A_k = \sum_{i=0}^{k} \left( \begin{array}{c} 2g \\ i \end{array} \right) \frac{q^{2k+2i-2} - 1}{q^2 - 1} q^i < h(F) q^{2k+2i-2g}.
\]

Proof. The formula of \(A_k\) follows directly from the formula of L-function of a maximal curve over \(\mathbb{F}_q^2\), which is \(L_F(T) = (1 + qT)^{2g}\), cf. [5]. Note that \(h(F) = L_F(1)\), thus one obtain the above inequality by some simple calculations. \(\Box\)

Combining Lemma 2.1, we yield the following result:

Proposition 2.3. Suppose \(F\) is a maximal curve over \(\mathbb{F}_q^2\) of genus \(g\) with at least \(n\) rational points and for some integers \(l\) and \(t\) holds

\[
\left( \begin{array}{c} n \\ l \end{array} \right) q^{2t+2-2g} \leq 1.
\]
Then there exists \([n, k, d]\) code over \(\mathbb{F}_{q^2}\) with \(k = l + t - g + 1\) and \(d \geq n - l + 1\).

By applying Proposition 2.3 we are ready to prove our main theorem.

**Theorem 2.4.** There exist \([n, k, d]\) linear codes over \(\mathbb{F}_{q^2}\) with \(k + d \geq n - 3\) for all sufficiently large \(n = q^3\), where \(q\) is a prime power.

**Proof.** Below we construct Hermitian codes over \(\mathbb{F}_{q^2}\) of sufficiently large length \(n = q^3\). Fix \(n\), we take \(l = \lfloor n\alpha \rfloor\), \(t = g - 1 + \lfloor (\theta - 1)l \rfloor\) for some \(0 < \theta, \alpha < 1\).

We compute
\[
\lim_{n \to \infty} \frac{\log_q \left(\binom{n}{2} q^{2t + 2 - 2g} \right)}{n} = -\alpha \log_q \left(1 - \frac{\alpha}{\alpha} \right) \log_q \left(1 - \frac{\alpha}{\alpha} \right) + 2\alpha(\theta - 1).
\]

To achieve that the above sum is negative, one must choose \(\theta < 1 - \log_{q^2} \frac{H_2(\alpha)}{2\alpha}\), where \(H_2(\delta) = -\delta \log_{\log_2} (1 - \delta) \log_2^{1-\delta}\) is the 2-th entropy function. Taking \(\theta = 1 - \log_{q^2} \frac{H_2(\alpha)}{2\alpha} - o(1)\) and \(\alpha = q^{-3+\varepsilon}\) for some positive \(\varepsilon = \varepsilon_q\) with \(\lim_{q \to \infty} q^\varepsilon \to 2\). By Proposition 2.3 we achieve the following inequalities

\[
dimproved := d - d_{\text{Goppa}} \geq g - 1 - \frac{\log_{q^2} H_2(\alpha)}{2\alpha} l - o(l)
\]

\[
= g - 1 + \frac{q^{-3+\varepsilon}}{2}(\varepsilon - 3) + \frac{q^\varepsilon}{2} \log_q \left(1 - q^{\varepsilon-3} - o(q^\varepsilon)\right)
\]

\[
= g - 1 + \frac{q^\varepsilon}{2}(\varepsilon - 3) + \frac{-2q^\varepsilon + q^{-3+2\varepsilon} + \ldots}{4 \ln q} - o(2)
\]

\[
= g - 4 - o(1).
\]

**Remark 2.5.** We set \(\lim_{q \to \infty} q^\varepsilon \to 2\) such that the codes we yield are not trivial codes. One can show that this value can be replaced by any value larger than one.

**Remark 2.6.** In [10, Remark 4.6], the improvement to Goppa’s construction for Hermitian codes is close to \(g - q\). Clearly, our construction yields codes with better parameters over large fields. We note that most results in this article work for any maximal curve.

**References**

[1] M. A. Tsfasman, S.G. Vladut, T. Zink, *Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound*. Math. Nachr. 109 (1982), 21–28.

[2] N.D. Elkies, *Excellent nonlinear codes from modular curves*. In STOC 01: Proceedings of the 33rd Annual ACM Symposium on Theory of Computing, (2001), 200–208.

[3] N.D. Elkies, *Still better nonlinear codes from modular curves*. http://arxiv.org/abs/math/0308046

[4] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer Universitext, Berlin-Heidelberg, 1993.
[5] H. Niederreiter and C.P. Xing, *Rational Points on Curves over Finite Fields: Theory and Applications*. Cambridge University Press, Cambridge, 2001.

[6] M.A. Tsfasman and S.G. Vladut, *Algebraic-Geometric Codes*. Dordrecht, The Netherlands: Kluwer, 1991.

[7] C.P. Xing, *Algebraic geometry codes with asymptotic parameters better than the Gilbert-Varshamov and the Tsfasman-Vladut-Zink bounds*. IEEE Trans. Inf. Theory, 47 (2001), 347–352.

[8] C.P. Xing, *Nonlinear codes from algebraic curves improving the Tsfasman-Vladut-Zink bound*. IEEE Trans. Inf. Theory, 49 (2003), 432–437.

[9] C.P. Xing and H. Chen, *Improvements on parameters of one-point AG codes from Hermitian curves*. IEEE Trans. Inf. Theory, 48 (2002), 535–537.

[10] L. Xu, *Improvement on parameters of Goppa geometry codes from maximal curves using the Vladut-Xing method*. IEEE Trans. Inf. Theory, 51 (2005), 2207–2210.

[11] K. Yang and P.V. Kumar, *On the true minimum distances of Hermitian codes*. In Lecture Notes in Mathematics. vol. 1518, pp. 99–107, 1991.

Siman Yang
Department of Mathematics, East China Normal University,
500, Dongchuan Rd., Shanghai, P.R.China 200241. e-mail: smyang@math.ecnu.edu.cn