On the Nonexistence of q-ary Linear Codes Attaining the Griesmer Bound*

Xiuli Li†

Department of Mathematics, Shanghai Jiao Tong University, Shanghai 200240, China

School of Math. and Phys., Qingdao University of Science and Technology, Qingdao 266061, China

Abstract. In this paper, we will prove that there exist no $[n, k, d]_q$ codes for $sq^{k-1} - (s+t)q^{k-2} - q^{k-4} \leq d \leq sq^{k-1} - (s+t)q^{k-2}$ attaining the Griesmer bound with $k \geq 4$, $1 \leq s \leq k-2$, $t \geq 1$ and $s+t \leq (q+1)/2$. Furthermore, we will prove that there exist no $[n, k, d]_q$ codes for $sq^{k-1} - (s+t)q^{k-2} - q^{k-3} + 1 \leq d \leq sq^{k-1} - (s+t)q^{k-2}$ attaining the Griesmer bound with $k \geq 3$, $1 \leq s \leq k-2$, $t \geq 1$ and $s+t \leq \sqrt{q} - 1$. The results generalize the nonexistence theorems of Tatsuya Maruta (see [7]) and Andreas Klein (see [4]) to a larger class of code.

Keywords: linear codes, Griesmer bound, projective spaces, extension of linear codes

MSC: 94B27, 94B05, 51E22, 51E21

1 Introduction

We denote by $GF(q)$ the Galois field of order q. An $[n, k, d]_q$ code is a linear code of length n with dimension k whose minimum Hamming distance is d over $GF(q)$. One of the central problems in coding theory is to determine $n_q(k, d)$, the minimum value of n for which there exists an $[n, k, d]_q$ code for given q, k, d. As a lower bound on $n_q(k, d)$ the following is well known .

Theorem 1.1 (*The Griesmer bound* – see[2], [8])

*Research supported by scientific research start-up foundation of Qingdao University of Science and Technology in China.

† *E-mail: lixiuli2004@tom.com*

$$n_q(k,d) \geq g_q(k,d) := \sum_{i=0}^{k-1} \lceil d/q^i \rceil,$$

where $\lceil x \rceil$ *denotes the smallest integer greater than or equal to* x.

It is known that $n_q(k,d) = g_q(k,d)$ for all d, $k = 1,2$ and for $d \geq (k-2)q^{k-1} - (k-1)q^{k-2} + 1$, $k \geq 3$ for all q (see [3], [7]). For $d = (k-2)q^{k-1} - (k-1)q^{k-2}$, $k \geq 3$, S.M. Doudunekov (see [1]), R. Hill (see [3]) and T. Maruta (see [6], [7]) have given the following theorem.

Theorem 1.2 *For* $d = (k-2)q^{k-1} - (k-1)q^{k-2}$, $n_q(k,d) > g_q(k,d)$ *holds for* $q \geq k$, $k = 3,4,5$ *and* $q \geq 2k-3$, $k \geq 6$.

In the paper [5], the author obtained the following theorem.

Theorem 1.3 *For* $d = mq^{k-1} - (m+1)q^{k-2}$, $n_q(k,d) > g_q(k,d)$ *holds for* $1 \leq m \leq k-2$, $q \geq m+2$, $k = 3,4,5$ *and* $q > 2m$, $k \geq 6$.

Let C be an $[n,k,d]_q$ code with a generator matrix M. The code obtained by deleting the same coordinate from each codeword of C is called a *punctured code* of C. If there exists an $[n+1,k,d+1]_q$ code C' which gives C as a punctured code, C is called *extendable* (to C') and C' is an *extension* of C. By extension of linear codes, Andreas Klein (see [4]) has proved the following theorem.

Theorem 1.4 *There exist no* $[g_q(k,d),k,d]_q$ codes *if* $q \geq 2k-3$, $k \geq 4$ *and*

$$(k-2)q^{k-1} - (k-1)q^{k-2} - q^{k-4} \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}.$$

Furthermore, if $q \geq k^2+k-1$, *then there exist no* $[g_q(k,d),k,d]_q$ *codes with* $k \geq 3$ *and*

$$(k-2)q^{k-1} - (k-1)q^{k-2} - q^{k-3} + 1 \leq d \leq (k-2)q^{k-1} - (k-1)q^{k-2}.$$

In this paper, we will generalize the above results and obtain the following Theorems.

Theorem 1.5 *There exist no* $[g_q(k,d),k,d]_q$ *codes if* $k \geq 4$, $1 \leq s \leq k-2$, $t \geq 1$, $s+t \leq (q+1)/2$ *and*

$$sq^{k-1} - (s+t)q^{k-2} - q^{k-4} \leq d \leq sq^{k-1} - (s+t)q^{k-2}.$$

Theorem 1.6 *There exist no* $[g_q(k,d),k,d]_q$ *codes if* $k \geq 3$, $1 \leq s \leq k-2$, $t \geq 1$, $s+t \leq \sqrt{q}-1$ *and*

$$sq^{k-1}-(s+t)q^{k-2}-q^{k-3}+1 \leq d \leq sq^{k-1}-(s+t)q^{k-2}.$$

2 Geometric preliminaries

Assume that $k \geq 3$. We denote by $\Sigma = PG(k-1,q)$ the projective space of dimension $k-1$ over $GF(q)$. A j-flat is a projective subspace of dimension j in Σ. 0-flats, 1-flats, 2-flats and $(k-2)$-flats are called *points*, *lines*, *planes* and *hyperplanes* respectively. Denote by θ_j the number of points in a j-flat, i.e. $\theta_j = (q^{j+1}-1)/(q-1)$. We set $\theta_{-1} = 0$ for convenience.

Let C be an $[n,k,d]_q$ code which does not have any coordinate position in which all the codewords have a zero entry. The columns of a generator matrix M of C can be considered as a multiset of n points in Σ denoted by $\overline{M}$. An *i-point* is a point which has multipicity i in $\overline{M}$. Let C_i be the set of i-points in Σ. Let γ_0 be the maximum number of i for which an i-point exists in Σ. For any subset S of Σ, we define

$$c_0(S) = max\{i \mid S \cap C_i \neq \emptyset\},$$

$$c(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|,$$

where $|T|$ denotes the number of points in T for a subset T of Σ. Define $\gamma_j = max\{c(\Delta) \mid \Delta \text{ is a } j\text{-flat in } \Sigma\}$, $1 \leq j \leq k-1$. Then $\gamma_{k-2} = n-d$ holds (see [3]). Hence we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ such that

$$c(\Sigma) = n,$$
$$c(\pi) \leq n-d \text{ for any hyperplane } \pi \text{ of } \Sigma,$$
$$c(\pi) = n-d \text{ for some hyperplane } \pi \text{ of } \Sigma.$$

Conversely such a partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ as above gives an $[n,k,d]_q$ code in the natural way if there exists no hyperplane containing the complement of C_0 in Σ. When C attains the Griesmer bound, $\gamma_0, \gamma_1, \cdots, \gamma_{k-3}$ are uniquely determined as follows.

Theorem 2.1 (see [7]) *Let* C *be an* $[n,k,d]_q$ *code attaining the Griesmer bound. Then it holds that*

$$\gamma_j = \sum_{u=0}^{j} \left\lceil \frac{d}{q^{k-1-u}} \right\rceil \text{ for } 0 \leq j \leq k-1.$$

Let a_i be the number of hyperplanes π of Σ with $c(\pi) = i$. An easy counting argument yields that

Theorem 2.2 (see [6]) *If $a_i = 0$ for all $i < n - d$, then θ_{k-1} divides n, and $\Sigma = C_s$ holds, where $s = n/\theta_{k-1}$.*

3 Main Theorems

Let C be an $[n, k, d]_q$ code attaining the Griesmer bound for $d = sq^{k-1} - (s+t)q^{k-2}$ with $k \geq 4$, $1 \leq s \leq k-2$, $t \geq 1$ and $s + t \leq (q + 1/)2$. Then we have $n = g_q(k, d) = sq^{k-1} - t\theta_{k-2}$. Let $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ be the partition derived from a generator matrix of C.

Lemma 3.1 (1) $\gamma_j = sq^j - t\theta_{j-1}$ *for* $0 \leq j \leq k-1$.
(2) *Δ is a j-flat with $c(\Delta) = \gamma_j$ if and only if $c_0(\Delta) = s$ for $0 \leq j \leq k-1$.*

Proof. (1) The results are straightforward from Theorem 2.1.
(2) Obviously it is true for $j = 0$ or $j = k-1$. It follows from (1) that $\gamma_0 = s$ and $\gamma_1 = sq - t$. Since $n = (sq - t - s)\theta_{k-2} + s$, then every line l containing an s -point satisfies $c(l) = sq - t = \gamma_1$. Let l be a line with $c(l) = \gamma_1$. If $l \cap C_s = \emptyset$, then $\gamma_1 \leq (s-1)(q+1) < sq - t$, a contradiction. Hence we have $c_0(l) = s$.
Let Δ be a j-flat with $c_0(\Delta) = s$, $2 \leq j \leq k-2$. Then

$$c(\Delta) = (\gamma_1 - s)\theta_{j-1} + s = sq^j - t\theta_{j-1} = \gamma_j.$$

Conversely, let Δ be a j-flat with $c(\Delta) = \gamma_j$, $2 \leq j \leq k-2$. If $\Delta \cap C_s = \emptyset$, then $\gamma_j \leq (s-1)\theta_j < sq^j - t\theta_{j-1}$, a contradiction. Hence we have that $c_0(\Delta) = s$. □

Lemma 3.2 *Let Δ be a plane with $c(\Delta) = \gamma_2$ and let l_1, l_2 be two distinct lines on Δ with $t_0 = c(l_1 \cap l_2)$, $t_i = c(l_i)$, $i = 1, 2$. Then*

$$t_1 + t_2 \geq sq + qt_0 - 2t.$$

Proof. The assertion follows from

$$\gamma_2 \leq t_1 + t_2 - t_0 + (q-1)(\gamma_1 - t_0).$$

Lemma 3.3 (1) $c_0(l) > 0$ *for any line l of Σ.*

(2) *Let l be a line of Σ with $c_0(l) = r$, $1 \le r \le s$. Then $c(l) = rq - t$.*

Proof. (1) Suppose that there exists a line l_0 included in C_0. Take a plane Δ containing l_0 and an s-point. Setting $t_0 = t_1 = 0$ in Lemma 3.2, we have $t_2 \ge sq - 2t > (s-1)q$. Hence every line l ($\neq l_0$) on Δ contains an s-point and so $c(l) = \gamma_1$ by Lemma 3.1 (2). Considering the lines on Δ containing a fixed 0-point, we obtain $\gamma_2 = q\gamma_1$, a contradiction.

(2) In the case $r = s$ we have proved in Lemma 3.1 (2).

Next we assume that $r < s$. Let P be an s-point, π be the plane through P and l. Then $c(\pi) = sq^2 - t\theta_1$. Let l' be a line different from l in π with intersect l at an r-point. Since $c(l) \le r(q+1)$, then $c(l') \ge (sq^2 - t\theta_1) - rq - (q-1)(sq - t - r) = sq - 2t - r$. Since $2 \le s + t \le (q+1)/2$, we have $c(l') > (s-1)(q+1)$. Thus $c_0(l') = s$ and therefore $c(l') = sq - t$. We look at all lines in π through a fixed r-point of l. It easily follows that $c(l) = (sq^2 - t\theta_1) - q(sq - t - r) = rq - t$. □

Lemma 3.4 *Let π be a hyperplane of Σ with $c_0(\pi) = r$, $1 \le r \le s$. Then*

(1) $c(\pi) = rq^{k-2} - t\theta_{k-3}$.

(2) *For a j-flat Δ in π containing a r-point ($1 \le j \le k-2$), the partition $\Delta = \bigcup_{i=0}^{r}(\Delta \cap C_i)$ gives an $[rq^j - t\theta_{j-1}, j+1, rq^j - (r+t)q^{j-1}]_q$ code.*

Proof. (1) Let P be an r-point in π. Considering the lines in π through P, it follows from Lemma 3.3 (2) that $c(\pi) = (rq - t - r)\theta_{k-3} + r = rq^{k-2} - t\theta_{k-3}$.

(2) Let Δ be a j-flat in π containing an r-point P in π. Considering the lines in π through P, we obtain

$$c(\Delta) = (rq - t - r)\theta_{j-1} + r = rq^j - t\theta_{j-1}.$$

Similarly, $c(\Delta_0) = rq^{j-1} - t\theta_{j-2}$ for every $(j-1)$-flat Δ_0 in Δ containing a r-point. By Lemma 3.3 (2) we have $c(\Delta_0') \le rq^{j-1} - t\theta_{j-2}$ for every $(j-1)$-flat Δ_0' in Δ. Hence the partition $\Delta = \bigcup_{i=0}^{r}(\Delta \cap C_i)$ gives an $[rq^j - t\theta_{j-1}, j+1, rq^j - (r+t)q^{j-1}]_q$ code. □

Lemma 3.5 *For $d = q^2 - (t+1)q$, $n_q(3,d) > g_q(3,d)$ holds for $1 \le t \le (q-1)/2$.*

Proof. This is the case $k = 3$. Let C be an $[g_q(3,d), 3, d]_q$ code with $d = q^2 - (t+1)q$ and $1 \le t \le (q-1)/2$. Then we have $g_q(3,d) = q^2 - t\theta_1$. The columns of a generator M of C can be considered as a multiset of $q^2 - t\theta_1$ points in $\sigma = PG(2,q)$. From Theorem 2.1 it follows that $\gamma_0 = 1$,

$\gamma_1 = q - t$. Similarly as Lemma 3.3 (1) we have $c_0(l) > 0$ for every line l in σ. Hence $c_0(l) = 1$ and furthermore $c(l) = q - t$ for every line l in σ. Thus we have $(q^2 - t\theta_1)(q+1) = \theta_2(q-t)$, a contradiction.

Theorem 3.6 *There exist no* $[g_q(k,d),k,d]_q$ *codes with* $d = sq^{k-1} - (s+t)q^{k-2}$ *for* $k \geq 4$, $1 \leq s \leq k-2$, $t \geq 1$ and $s+t \leq (q+1)/2$.

Proof. When $k = 4$, we have $s = 1$, or 2. It follows from Lemmas 3.3 (1), 3.4 and 3.5 that there exists no hyperplane π of Σ with $c_0(\pi) < s$, contracting Theorem 2.2. Hence there exist no $[g_q(4,d),4,d]_q$ codes with $d = sq^2 - (s+t)$ Using induction on k we also get a contradiction for $k \geq 5$. This completes the proof.

Andreas Klein have given the following two results of extending codes.

Lemma 3.7(see [4]) *Let* $s+t < q$ *and* $k \geq 4$. *Each* $[g_q(k,d),k,d]_q$ *code with*

$$sq^{k-1} - (s+t)q^{k-2} - q^{k-4} \leq d < sq^{k-1} - (s+t)q^{k-2}$$

can be extended to a $[g_q(k,d'),k,d']_q$ *code with* $d' = sq^{k-1} - (s+t)q^{k-2}$.

Lemma 3.8(see [4]) *Let* $(s+t)^2+3(s+t)+1 \leq q$, *then each* $[g_q(k,d),k,d]_q$ *code with*

$$sq^{k-1} - (s+t)q^{k-2} - q^{k-3} + 1 \leq d < sq^{k-1} - (s+t)q^{k-2}$$

and $k \geq 3$ *can be extended to a* $[g_q(k,d'),k,d']_q$ *code with* $d' = sq^{k-1} - (s+t)q^{k-2}$.

In fact, the condition $(s+t)^2+3(s+t)+1 \leq q$ in Lemma 3.8 can be improved to $(s+t+1)^2 \leq q$. We only need to substitute $(q-s-t)/(s+t+1) > (s+t)$ for $(q-s-t)/(s+t+1) \geq (s+t+1)$ in the proof of Theorem 10 in the paper [4]. Thus we have

Lemma 3.9 *Let* $s+t \leq \sqrt{q} - 1$, *then each* $[g_q(k,d),k,d]_q$ *code with*

$$sq^{k-1} - (s+t)q^{k-2} - q^{k-3} + 1 \leq d < sq^{k-1} - (s+t)q^{k-2}$$

and $k \geq 3$ *can be extended to a* $[g_q(k,d'),k,d']_q$ *code with* $d' = sq^{k-1} - (s+t)q^{k-2}$.

Together with Theorem 3.6, Lemmas 3.7 and 3.9 yields the following nonexistence theorems, which we have mentioned in the introduction.

Theorem 1.5 *There exist no* $[g_q(k,d),k,d]_q$ *codes if* $k \geq 4$, $1 \leq s \leq k-2$, $t \geq 1$, $s+t \leq (q+1)/2$ *and*

$$sq^{k-1} - (s+t)q^{k-2} - q^{k-4} \leq d \leq sq^{k-1} - (s+t)q^{k-2}.$$

Theorem 1.6 *There exist no* $[g_q(k,d),k,d]_q$ *codes if* $k \geq 3$, $1 \leq s \leq k-2$, $t \geq 1$, $s+t \leq \sqrt{q}-1$ *and*

$$sq^{k-1} - (s+t)q^{k-2} - q^{k-3} + 1 \leq d \leq sq^{k-1} - (s+t)q^{k-2}.$$

References

[1] S.M. Doudunekov, On the achievement of the Solomon-Stiffler bound, *Comptes Rendus de l'Academie Bulgare des Sciences*, Vol. 39, 1986, pp. 39-41.

[2] J.H. Griesmer, A bound for error-correcting codes, *IBM J. Res. Develop.*, Vol. 4, 1960, pp. 532-542.

[3] R. Hill, Optimal linear codes, Proc. 2nd IMA Conf. on Cryptography and coding (C. Mitchell ed.), Oxford University Press, Oxford, 1992, pp. 75-104.

[4] A. Klein, On codes meeting the Griesmer bound, *Discrete Math.*, Vol. 274, 2004, pp. 289-297.

[5] Xiuli Li, On the minimum length of q-ary linear codes, submitted to Chinese Annals of Mathematics (B).

[6] T. Maruta, On the nonexistence of linear codes of dimension four attaining the Griesmer bound, Proceedings of the International Workshop on Optimal Codes and Related Topics, Sozopol, Bulgaria, 1995, pp. 117-120.

[7] T. Maruta, On the achievement of the Griesmer bound, *Des. Codes Cryptogr.*, Vol. 12, 1997, pp. 83-87.

[8] G. Solomon and J.J. Stiffler, Algebraically punctured cyclic codes, *Inform. and Control*, Vol. 8, 1965, pp. 170-179.