A Remark on Linear Codes

Dan Dumitru
Faculty of Mathematics and Informatics
Spiru Haret University
Bucharest, Romania
dandumitru1984@yahoo.com

Abstract
The aim of this paper is to give an obstruction to the existence of $[n,k,d]$-linear codes. We prove in particular that there are no $[2k+1,k,k+1]$-binary linear codes for every $k \geq 4$. For the ternary case we prove in particular that there are no $[3k+1,k,2k+1]$-ternary linear codes for every $k \geq 3$. We also prove that there is no linear code C over $\mathbb{F}_q$ of parameters $[qk,k,(q-1)k+1]$ for every $k \geq 2$.
Keywords: *Linear codes, Binary codes.*
ACM/AMS Classification: 94B05

1. Introduction

The study of the existence of certain linear codes has been a main topic in the code theory for many years and bounds to linear or non-linear codes have been given during the time ([1], [2], [3]). In this article we give some results about the non-existence of linear codes starting from the well-known Griesmer and Singleton's bounds. We will first consider the following notations: $\mathbb{F}_q$ is the finite field of q elements and C is a linear code of parameters $[n,k,d]$, which means the codewords of C have length n, C has dimension k and the minimum distance is $d = \min_{c \in C} wt(c)$, where by $wt(c)$ we have denoted the Hamming weight of a codeword $c \in C$.

The following two theorems about the existence of a code are well-known.

Theorem 1. *([2], [3], Griesmer's bound) Let C be a linear code over $\mathbb{F}_q$ of parameters $[n,k,d]$. Then $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$, where $\lceil x \rceil$ is the smallest integer greater than x.*

Theorem 2. *([1], Singleton's bound) For $q,n,d \in \mathbb{N}$, $q \geq 2$ it holds that $A(n,d) \leq q^{n-d+1}$, where $A(n,d) = \max\{M \in \mathbb{N} |$ an $[n,M,d]$code exists$\}$. In particular for a linear code C over $\mathbb{F}_q$ of parameters $[n,k,d]$, we have $k+d \leq n+1$.*

2. **Main results**

We can state now the main results using the above two theorems.

Theorem 3. *Let the parameters* $[n, k, d]$ *be such that* $n, k, d \geq 1$ *and* $q \geq 2$.

(i) *Suppose* $q = 2$ *and* $n = 2k + 1$. *Then there is no linear code* C *over* $\mathbb{F}_q$ *if:*

$$\begin{cases} d \geq k+3, & \text{for every } k \geq 1 \\ d = k+2, & \text{for every } k \geq 2 \\ d = k+1, & \text{for every } k \geq 4 \end{cases}$$

(ii) *Suppose* $q \geq 3$ *and* $n = qk + 1$. *Then there is no linear code* C *over* $\mathbb{F}_q$ *if:*

$$\begin{cases} d \geq (q-1)k+3, & \text{for every } k \geq 1 \\ d = (q-1)k+2, & \text{for every } k \geq 2 \\ d = (q-1)k+1, & \text{for every } k \geq 3 \end{cases}$$

Proof:

(i) Let $q = 2$ and $n = 2k + 1$.

a) If $d \geq k + 3$, then $k + d \geq 2k + 3 > 2k + 2 = n + 1$ and thus from Singleton's bound there is no linear code C.

b) If $d = k + 2$, then:

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil = \sum_{i=0}^{k-1} \left\lceil \frac{k+2}{2^i} \right\rceil \geq \sum_{i=0}^{k-1} \frac{k+2}{2^i} = (k+2) \sum_{i=0}^{k-1} \frac{1}{2^i} =$$
$$= (k+2) \cdot \frac{2^k - 1}{2^{k-1}} > 2k+1 \iff$$
$$\iff (k+2)(2^k - 1) > (2k+1)2^{k-1} \iff 2^k > 2^{k-1} + k + 2$$

inequality which is true by induction for every $k \geq 2$ and thus from Griesmer's bound there is no linear code C.

c) If $d = k + 1$, then:

$$\sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil = \sum_{i=0}^{k-1} \left\lceil \frac{k+1}{2^i} \right\rceil \geq \sum_{i=0}^{k-1} \frac{k+1}{2^i} = (k+1) \sum_{i=0}^{k-1} \frac{1}{2^i} =$$
$$= (k+1) \cdot \frac{2^k - 1}{2^{k-1}} > 2k+1 \iff$$
$$\iff (k+1)(2^k - 1) > (2k+1)2^{k-1} \iff 2^k > 2^{k-1} + k + 1$$

inequality which is true by induction for every $k \geq 4$ and thus from Griesmer's bound there is no linear code C.

(ii) Let $q \geq 3$ and $n = qk + 1$.

a) If $d \geq (q-1)k + 3$, then $k + d \geq qk + 3 > qk + 2 = n + 1$ and thus from Singleton's bound there is no linear code C.

b) If $d = (q-1)k+2$, then:

$$\sum_{i=0}^{k-1}\left\lceil \frac{d}{q^i}\right\rceil = \sum_{i=0}^{k-1}\left\lceil \frac{(q-1)k+2}{q^i}\right\rceil \geq \sum_{i=0}^{k-1}\frac{(q-1)k+2}{q^i} = [(q-1)k+2]\sum_{i=0}^{k-1}\frac{1}{q^i} =$$
$$= [(q-1)k+2]\cdot\frac{q^k-1}{q^{k-1}(q-1)} > qk+1 \Longleftrightarrow$$
$$\Longleftrightarrow [(q-1)k+2](q^k-1) > (qk+1)q^{k-1}(q-1) \Longleftrightarrow$$
$$\Longleftrightarrow (q+1)q^{k-1} > (q-1)k+2$$

inequality which is true by induction for every $k \geq 2$ and thus from Griesmer's bound there is no linear code C.

c) If $d = (q-1)k+1$, then:

$$\sum_{i=0}^{k-1}\left\lceil \frac{d}{q^i}\right\rceil = \sum_{i=0}^{k-1}\left\lceil \frac{(q-1)k+1}{q^i}\right\rceil \geq \sum_{i=0}^{k-1}\frac{(q-1)k+1}{q^i} = [(q-1)k+1]\sum_{i=0}^{k-1}\frac{1}{q^i} =$$
$$= [(q-1)k+1]\cdot\frac{q^k-1}{q^{k-1}(q-1)} > qk+1 \Longleftrightarrow$$
$$\Longleftrightarrow [(q-1)k+1](q^k-1) > (qk+1)q^{k-1}(q-1) \Longleftrightarrow$$
$$\Longleftrightarrow q^{k-1} > (q-1)k+1$$

inequality which is true by induction for every $k \geq 3$ and thus from Griesmer's bound there is no linear code C.

In particular from theorem 3 we have the following two results:

Theorem 4. *There is no* $[2k+1, k, k+1]$*-binary linear code for every* $k \geq 4$.

Theorem 5. *There is no* $[3k+1, k, 2k+1]$*-ternary linear code for every* $k \geq 3$.

Moreover, we can extend theorem 3 to the following:

Theorem 6. *Let the parameters* $[n, k, d]$ *be such that* $n, k, d \geq 1$ *and* $q \geq 2$. *Then there is no linear code* C *over* $\mathbb{F}_q$ *of parameters* $[qk, k, (q-1)k+1]$ *for every* $k \geq 2$.

Proof: We have the following inequality:

$$\sum_{i=0}^{k-1}\left\lceil \frac{d}{q^i}\right\rceil = \sum_{i=0}^{k-1}\left\lceil \frac{(q-1)k+1}{q^i}\right\rceil \geq \sum_{i=0}^{k-1}\frac{(q-1)k+1}{q^i} = [(q-1)k+1]\sum_{i=0}^{k-1}\frac{1}{q^i} =$$
$$= [(q-1)k+1]\cdot\frac{q^k-1}{q^{k-1}(q-1)} > qk \Longleftrightarrow$$
$$\Longleftrightarrow [(q-1)k+1](q^k-1) > kq^{k+1} - kq^k \Longleftrightarrow q^k > (q-1)k+1$$

which is true for every $k \geq 2$.

In particular from theorem 6 we have the following two results:

Theorem 7. *There is no* $[2k, k, k+1]$*-binary linear code for every* $k \geq 2$.

Theorem 8. *There is no* $[3k, k, 2k+1]$*-ternary linear code for every* $k \geq 2$..

Remark 9. Theorems 7 and 8 are not true for $k = 1$ as one can see from below:

1) $C = \{00, 11\}$ is a $[2, 1, 2]$-binary linear code.

2) $C = \{000, 111, 222\}$ is a $[3, 1, 3]$-ternary linear code.

Moreover, if we consider the $[2k, k, k]$-binary linear codes and $[3k, k, 2k]$-ternary linear codes we have:

3) If $k = 1$, $C = \{00, 01\}$ is a $[2, 1, 1]$-binary linear code.

3) If $k = 2$, $C = \{0000, 0011, 1100, 1111\}$ is a $[4, 2, 2]$-binary linear code.

3) If $k = 3$,

$$C = \{000000, 111000, 011100, 001110, 100100, 110110, 010010, 101010\}$$

is a $[6, 3, 3]$-binary linear code.

3) If $k = 1$, $C = \{000, 011, 022\}$ is a $[3, 1, 2]$-ternary linear code.

Remark 10.

a. Regarding theorem 3, point i) there exist binary linear codes for $k \leq 3$ such as:

1) If $k = 1$ we have $C = \{000, 111\}$ a $[3, 1, 3]$-binary linear code and $C = \{000, 011\}$ a $[3, 1, 2]$-binary linear code.
2) If $k = 2$ we have $C = \{00000, 00111, 11100, 11011\}$ a $[5, 2, 3]$-binary linear code.
3) If $k = 3$ we have

$$C = \{0000000, 0001111, 0110011, 0111100, 1100110, 1101001, 1010101, 1011010\}$$

a $[7, 3, 4]$-binary linear code.

b. Regarding theorem 3, point ii) there exist ternary linear codes for $k \leq 2$ such as:

1) If $k = 1$ we have $C = \{0000, 1111, 2222\}$ a $[4, 1, 4]$-ternary linear code and $C = \{0000, 0111, 0222\}$ a $[4, 1, 3]$-ternary linear code.
2) If $k = 2$ we have

$$C = \{000000, 0011111, 0022222, 1110012, 2220021, 1102201, 2201102, 1121120, 2212210\}$$

a $[7, 2, 5]$-ternary linear code.

c. If we consider the case of the binary linear codes of the type $[2k + 1, k, k]$, $k \geq 1$, one can have the following examples:

1) $C = \{000, 100\}$ is a $[3, 1, 1]$-binary linear code.
2) $C = \{00000, 11000, 01100, 10100\}$ is a $[5, 2, 2]$-binary linear code.

3)

$$C = \{0000000, 1110000, 0011100, 0000111, 1101100, \\ 1110111, 0011011, 1101011\}$$

is a $[7, 3, 3]$-binary linear code.

4)

$$C = \{000000000, 111100000, 001111000, 000011110, 101010100, \\ 110011000, 001100110, 111111110, 110000110, 010110100, 100101100, \\ 101001010, 011001100, 100110010, 010101010, 011010010\}$$

is a $[9, 4, 4]$-binary linear code

d. If we consider the case of the ternary linear codes of the type $[3k+1, k, 2k]$, $k \geq 1$, one can have the following examples:

1) $C = \{0000, 1100, 2200\}$ is a $[4, 1, 2]$-ternary linear code.

2)

$$C = \{0000000, 0001111, 0002222, 1110002, 2220001, 1111110, \\ 2222220, 1112221, 2221112\}$$

is a $[7, 2, 4]$-ternary linear code.

References

1. S. Ling, C. Xing, *Coding Theory - A first course*, Cambridge University Press, 2004.
2. J.H. Griesmer, *A bound for error-correcting codes*, IBM J. Res. Dev.4, 1960, 532-542.
3. G. Solomon, J.J. Stiffler, *Algebraically punctured cyclic codes*, Inf. Control 8, 1965, 170-179.