On the Griesmer bound for nonlinear codes

Emanuele Bellini, Alessio Meneghetti

On the Griesmer bound for nonlinear codes

Emanuele Bellini[1] and Alessio Meneghetti[2]

[1] Telsy S.p.A., Italy
eemanuele.bellini@gmail.com
[2] University of Trento, Italy
almenegh@gmail.com

Abstract. Most bounds on the size of codes hold for any code, whether linear or nonlinear. Notably, the Griesmer bound holds only in the linear case. In this paper we identify code parameters (q, d, k) for which the Griesmer bound holds also in the (systematic) nonlinear case. Moreover, we show that the Griesmer bound does not necessarily hold for a systematic code by showing explicit counterexamples. On the other hand, we are also able to provide some versions of the Griesmer bound holding for all systematic codes.

1 Introduction

We consider codes over a finite field $\mathbb{F}_q$ of length n, with M codewords, and distance d. A code C with such parameters is denoted as an $(n, M, d)_q$-code.

Definition 1. *An $(n, q^k, d)_q$-systematic code C is the image of a map $F : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$, $n \geq k$, s.t. a vector $x = (x_1, \ldots, x_k) \in (\mathbb{F}_q)^k$ is mapped to a vector*

$$(x_1, \ldots, x_k, f_{k+1}(x), \ldots, f_n(x)) \in (\mathbb{F}_q)^n,$$

where $f_i,\ i = k+1, \ldots, n$, are maps from $(\mathbb{F}_q)^k$ to $\mathbb{F}_q$. We refer to k as the dimension of C. The coordinates from 1 to k are called systematic, while those from $k+1$ to n are called non-systematic.

If the maps f_i are all linear, then the systematic code C is a subspace of dimension k of $(\mathbb{F}_q)^n$ and we say it is a $[n, k, d]_q$-linear code. A nonlinear code is a code that is not necessarily linear or systematic.
We denote with $\mathrm{len}(C), \dim(C), \mathrm{d}(C)$, respectively, the length, the dimension (when defined) and the minimum distance of a code C.
Recent results on systematic codes can be found in [AB08] and [AG09], where it is proved that if a linear code admits an extension, then it admits also a linear extension.

This implies that if a systematic code C can be puntured obtaining a linear code, then there exists a linear code with the same parameters of C.
A central problem of coding theory is to determine the minimum value of n for which an $(n, M, d)_q$-code or an $[n, k, d]_q$-linear code exists. We denote by $N_q(M, d)$ the minimum length of a nonlinear code over $\mathbb{F}_q$, with M codewords and distance d. We denote by $S_q(k, d)$ the same value in the case of a systematic code of dimension k, while we use $L_q(k, d)$ in the case of a linear code of dimension k. Observe that

$$N_q\left(q^k, d\right) \leq S_q(k, d) \leq L_q(k, d).$$

A well-known lower bound for $L_q(k, d)$ is

Theorem 1 (Griesmer bound). *All $[n, k, d]_q$ linear codes satisfy the following bound:*

$$n \geq L_q(k, d) \geq g_q(k, d) := \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \tag{1}$$

The Griesmer bound was introduced by Griesmer [Gri60] in the case of binary linear codes and then generalized by Solomon and Stiffler [SS65] in the case of q-ary linear codes. It is known that the Griesmer bound is not always sharp [Van80].
Important examples of linear codes meeting the Griesmer bound are the simplex code [HP03] (Section 1.8) and the $[5, 6, 11]_3$ Golay code [HP03] (Section 1.9).
Many authors such as [Mar97] and [Kle04], have identified classes of linear codes meeting the Griesmer bound. In particular, finite projective geometries play an important role in the study of these codes. Many known bounds on the size of nonlinear codes, for example the Johnson bound ([Joh71]), the Plotkin bound ([Plo60], the Bellini-Guerrini-Sala bound ([BGS14]) and the Linear Programming bound ([Del73]), are true for both linear and nonlinear codes.

2 When the Griesmer bound holds for systematic codes

The following proposition and lemma are well-known.

Proposition 1. *Let C be an $(n, q^k, d)_q$-systematic code, and C' be the code obtained by shortening C in a systematic coordinate. Then C' is an $(n-1, q^{k-1}, d')_q$-systematic code with $d' \geq d$.*

Lemma 1. *If $n > k$, then given an $(n, q^k, d)_q$-systematic code C, there exists an $(n, q^k, \bar{d})_q$-systematic code $\bar{C}$ for any $1 \leq \bar{d} \leq d$.*

Theorem 2. *For fixed q and d, if*

$$S_q(k,d) \geq g_q(k,d) \tag{2}$$

for all k such that $1 \leq k < 1 + \log_q d$, then (2) *holds for any positive k.*

Proof. It is sufficient to show that if an $(n, q^k, d)_q$-systematic code not satisfying the Griesmer bound exists, then an $(n', q^{k'}, d)_q$-systematic code not satisfying the Griesmer bound exists with $k' < 1 + \log_q d$, and $n' > k'$.
For each fixed d, q suppose there exists k such that $S_q(k,d) < g_q(k,d)$. Let us call $\Lambda_{q,d} = \{k \geq 1 \mid S_q(k,d) < g_q(k,d)\}$. If $\Lambda_{q,d}$ is empty then the Griesmer bound is true for such parameters q, d. Otherwise there exists a minimum $k' \in \Lambda_{q,d}$ such that $S_q(k',d) < g_q(k',d)$. In this case we can consider an $(n, q^{k'}, d)_q$ systematic code C with $n = S_q(k',d)$. We build a new code C' by shortening C in a systematic coordinate. Clearly, C' is an $(n-1, q^{k'-1}, d')_q$ systematic code and $d' \geq d$. Applying Lemma 1 to C', we can obtain an $(n-1, q^{k'-1}, d)_q$ systematic code $\bar{C}$. Since k' was the minimum among all the values in $\Lambda_{q,d}$, the Griesmer bound holds for $\bar{C}$, and so

$$n - 1 \geq g_q(k'-1, d) = \sum_{i=0}^{k'-2} \left\lceil \frac{d}{q^i} \right\rceil . \tag{3}$$

We observe that, if $q^{k'-1} \geq d$, then $\left\lceil \frac{d}{q^{k'-1}} \right\rceil = 1$, so we can rewrite (3) as

$$n \geq \sum_{i=0}^{k'-2} \left\lceil \frac{d}{q^i} \right\rceil + 1 \geq \sum_{i=0}^{k'-2} \left\lceil \frac{d}{q^i} \right\rceil + \left\lceil \frac{d}{q^{k'-1}} \right\rceil = \sum_{i=0}^{k'-1} \left\lceil \frac{d}{q^i} \right\rceil = g_q(k',d)$$

Since we supposed $n < g_q(k',d)$, we have reached a contradiction.

□

3 Set of parameters for which the Griesmer bound holds in the nonlinear case

In this section we identify several sets of parameters (q,d) for which the Griesmer bound holds for systematic codes.

Theorem 3. *If $d \leq 2q$ then $S_q(k,d) \geq g_q(k,d)$.*

Proof. First, consider the case $d \leq q$. By Theorem 2 it is sufficient to show that, fixing q, d, for any n an $(n, q^k, d)_q$-systematic code with $1 \leq k < 1 + \log_q d$ and $n < g_q(k,d)$

does not exist. If $1 \leq k < 1 + \log_q d$ then $\log_q d \leq \log_q q = 1$, and so k may only be 1. Since $g_q(1, d) = d$ and $n \geq d$, we clearly have that $n \geq g_q(1, d)$.
Now consider the case $q < d \leq 2q$. If $1 \leq k < 1 + \log_q d$ then $\log_q d \leq \log_q 2q = 1 + \log_q 2$, and so k can only be 1 or 2. We have already seen that if $k = 1$ then $n \geq g_q(k, d)$ for any n, so suppose $k = 2$. If an $(n, q^2, d)_q$-systematic code C exists with $n < \sum_{i=0}^{1} \left\lceil \frac{d}{q^i} \right\rceil = d+2$, then by the Singleton bound we can only have $n = d+1$. Therefore C must have parameters $(d + 1, q^2, d)$.
In [Hil86, Ch. 10] it is proved that a q-ary $(n, q^2, n-1)_q$ code is equivalent to a set of $n-2$ mutually orthogonal Latin squares (MOLS) of order q (Theorem 10.20), and that there are at most $q-1$ Latin squares in any set of MOLS of order q (Theorem 10.18). In our case $n = d + 1 > q + 1$, therefore $n - 2 > q - 1$. The existence of C would imply the existence of a set of more than $q-1$ MOLS, which is impossible.

□

Theorem 4 (Plotkin bound). *Consider an $(n, M, d)_q$ code, with M being the number of codewords in the code. If $n < \frac{qd}{q-1}$, then $M \leq d/(d - (1 - 1/q)n)$, or equivalently $n \geq d((1 - 1/M)/(1 - 1/q))$.*

Proposition 2. *Let r be a positive integer, then $N_q(q^k, q^{k-1}r) \geq g_q(k, q^{k-1}r)$.*

Proof. Suppose there exists an $(n, q^k, q^{k-1}r)_q$-code C that does not satisfy the Griesmer bound. Hence $n < \sum_{i=0}^{k-1} \left\lceil \frac{q^{k-1}r}{q^i} \right\rceil$. Observe that in this case $\sum_{i=0}^{k-1} \left\lceil \frac{q^{k-1}r}{q^i} \right\rceil = \sum_{i=0}^{k-1} \frac{q^{k-1}r}{q^i} = q^{k-1}r \sum_{i=0}^{k-1} \frac{1}{q^i}$. Since $\sum_{i=0}^{k-1} \frac{1}{q^i} = \frac{1-\frac{1}{q^k}}{1-\frac{1}{q}}$, we obtain

$$n < q^{k-1}r \left(\frac{1 - 1/q^k}{1 - 1/q} \right) . \tag{4}$$

We also observe that $n < q^{k-1}r \left((1 - 1/q^k)/(1 - 1/q) \right) < q^{k-1}r \left(1/(1 - 1/q) \right) = d/(1 - 1/q)$, and we can write this inequality as $n < \frac{dq}{q-1}$, which is the hypothesis for the Plotkin bound. Applying Theorem 4, we get $q^k \leq \left\lfloor \frac{d}{d-n(1-1/q)} \right\rfloor \leq \frac{d}{d-n(1-1/q)}$, i.e. $n \geq d \left(\frac{1-1/q^k}{1-1/q} \right)$, which contradicts equation (4). Hence each $(n, q^k, q^{k-1}r)_q$-code satisfies the Griesmer bound.

□

Note that Proposition 2 is not restricted to systematic codes, but it holds for nonlinear codes with at least q^k codewords, as the next corollary explains.

Corollary 1. *Let $M \geq q^k$ and let r be a positive integer. Then $N_q(M, q^{k-1}r) \geq g_q(k, q^{k-1}r)$.*

Lemma 2. *Let q be fixed, $d = q^l r$ for a certain r such that $1 \leq r < q$ and $l \geq 0$, and let k be such that $q^{k-1} \leq d$. Then $N_q(q^k, d) \geq g_q(k, d)$.*

Proof. Since $1 \leq r < q$, the hypothesis $q^{k-1} \leq d$ is equivalent to $k - 1 \leq l$. We use Proposition 4 and we set $h = \min(k-1, l)$, obtaining $n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$.

□

Theorem 5. *Let $1 \leq r < q$ and l a positive integer. Then $S_q(k, q^l r) \geq g_q(k, q^l r)$.*

Proof. To prove that the Griesmer bound is true for these particular choices of d we use Theorem 2, hence we only need to prove that the Griesmer bound is true for all choices of k such that $q^{k-1} \leq d$.
We now use Lemma 2, which ensures that all such codes respect the Griesmer bound.

□

Corollary 2. *Let $q = 2$ and let l be a positive integer, then $S_2(k, 2^l) \geq g_2(k, 2^l)$.*

We need the following numerical lemmas, whose proofs we omit and are present in [BGMS15].

Lemma 3. *Let r be a positive integer, and let $k \leq r+1$. Then $g_2(k, 2^{r+1}) = 2g_2(k, 2^r)$.*

Lemma 4. *For each k and d it holds*

$$g_2(k, d+1) = g_2(k, d) + \min(k, l+1), \tag{5}$$

where l is the maximum integer such that 2^l divides d.

Lemma 5. *If $k \leq r$, then $g_2(k, 2^r) < 2^{r+1}$.*

Theorem 6. *Let r and s be two positive integers such that $r > s$, and let $d = 2^r - 2^s$. Then $S_2(k, d) \geq g_2(k, d)$.*

Proof. If $r = s + 1$, then $2^r - 2^s = 2^s$, hence we can apply Corollary 2 and our claim holds. Therefore we can assume $r > s + 1$ in the rest of the proof. Suppose there exists $s < r$ s.t. $S_2(k, 2^r - 2^s) < g_2(k, 2^r - 2^s)$, i.e. the Griesmer bound does not hold for an $(n, 2^k, d)_2$-systematic code C, with $d = 2^r - 2^s$ and $n = S_2(k, d)$. Due to Theorem 2, we can consider the case $k < 1 + \log_2 d$, and so $k \leq r$. Let $m = n/d$. For C

$$m = \frac{S_2(k, 2^r - 2^s)}{2^r - 2^s} \leq \frac{g_2(k, 2^r - 2^s) - 1}{2^r - 2^s}$$

We claim that $m < g_2(k, 2^r)/(2^r)$. First we observe that if $k \leq r$, then

$$\frac{g_2(k, 2^r)}{2^r} = \sum_{i=0}^{k-1} \frac{1}{2^i} = 2\left(1 - \frac{1}{2^k}\right).$$

We consider now the ratio m:

$$m \leq \frac{g_2(k, 2^r - 2^s) - 1}{2^r - 2^s} = \frac{1}{2^r - 2^s} \sum_{i=0}^{k-1} \left\lceil \frac{2^r - 2^s}{2^i} \right\rceil - \frac{1}{2^r - 2^s} \tag{6}$$

We start from the case $k \leq s + 1$, and we can write (6) as

$$m < \frac{1}{2^r - 2^s} \sum_{i=0}^{k-1} \frac{2^r - 2^s}{2^i} = \sum_{i=0}^{k-1} \frac{1}{2^i} = 2\left(1 - \frac{1}{2^k}\right),$$

so $m < g_2(k, 2^r)/(2^r)$. We consider now the case $k > s+1$, and we write our claim in an equivalent way: $2^r(g_2(k, 2^r - 2^s) - 1) < (2^r - 2^s)g_2(k, 2^r)$. Rearranging the terms we obtain

$$2^s g_2(k, 2^r) < 2^r(g_2(k, 2^r) - g_2(k, 2^r - 2^s) + 1), \tag{7}$$

and we focus on the difference $g_2(k, 2^r) - g_2(k, 2^r - 2^s)$. For any d' in the range $2^r - 2^s \leq d' < 2^r$ we can apply Lemma 4, observing that $d' = 2^l r$ where $l \leq s$, and this implies $k > l + 1$. We obtain $g_2(k, d' + 1) = g_2(k, d') + l + 1$. Applying it for all distances from $2^r - 2^s$ till we reach 2^r we obtain

$$g_2(k, 2^r) - g_2(k, 2^r - 2^s) = 2^{s+1} - 1 \tag{8}$$

We substitute now (8) into (7), which becomes

$$2^s g_2(k, 2^r) < 2^r \cdot 2^{s+1} \qquad \Longrightarrow \qquad g_2(k, 2^r) < 2^{r+1},$$

and this is always true provided $k \leq r$, as shown in Lemma 5.

We now consider the $(tn, 2^k, td)_2$-systematic code C_t obtained by repeating t times the code C. We remark that the value m can be thought of as the slope of the line

$\mathrm{d}(C_t) \mapsto \mathrm{len}(C_t)$, and we proved that $m < g_2(k, 2^r)/(2^r)$. On the other hand, since $k \leq r$ we can apply Lemma 3, which ensures that $g_2(k, 2^{r+b}) = 2^b g_2(k, 2^r)$, namely the Griesmer bound computed on the powers of 2 is itself a line, and its slope is strictly greater than m. Due to this we can find a pair $(t,\ b)$ such that $td > 2^b$ and $tn < g_2(k, 2^b)$. This means that we can find a systematic code $\bar{C}$ with distance greater than 2^b and length smaller than $g_2(k, 2^b)$. We can apply Lemma 1, and find a systematic code with the same length of $\bar{C}$ and distance equal to 2^b. This contradicts Corollary 2, hence for each $k \leq r$ we have

$$S_2(k, 2^r - 2^s) \geq g_2(k, 2^r - 2^s).$$

Finally, observe that $k \leq r$ implies $k \leq \log_2(2^r) = \lceil \log_2(2^r - 2^s) \rceil < 1 + \log_2 d$, so we can apply Theorem 2 and conclude.

□

Corollary 3. *Let r and s be two positive integers such that $r > s$, and let $d = 2^r - 1$ or $d = 2^r - 2^s - 1$. Then $S_2(k, d) \geq g_2(k, d)$.*

Proof. We give the proof for the case $d = 2^r - 2^s - 1$, the same argument can be applied to the other case by applying Corollary 2 instead of Theorem 6.
Suppose $S_2(k, d) < g_2(k, d)$, i..e. there exists an $(n, k, d)_2$-systematic code for which

$$n < g_2(k, d). \tag{9}$$

We can extend such a code to an $(n+1, k, d+1)_2$-systematic code C by adding a parity check component to each codeword. Then C has distance $\mathrm{d}(C) = d + 1 = 2^r - 2^s$, so we can apply Theorem 6, finding $n + 1 \geq g_2(k, d + 1)$. Observe that d is odd, so applying Lemma 4 we obtain

$$n + 1 \geq g_2(k, d + 1) = g_2(k, d) + 1 \quad \Longrightarrow \quad n \geq g_2(k, d),$$

which contradicts (9).

□

4 Versions of the Griesmer bound holding for nonlinear codes

In this section we provide some versions of the Griesmer bound holding for any systematic code, whose proofs we omit and can be found in [BGMS15]. For systematic codes we can improve the Singleton bound as follows.

Proposition 3. *Let k and d be any positive integers, then*

$$S_2(k,d) \geq k + \left\lceil \frac{3}{2} d \right\rceil - 2.$$

We derive from Theorem 5 a weaker version of the Griesmer bound holding for any systematic code.

Remark 1. Considering an integer d, there exist $1 \leq r < q$ and $l \geq 0$ such that

$$q^l r \leq d < q^l (r+1) \leq q^{l+1}. \tag{10}$$

In particular, l has to be equal to $\lfloor \log_q d \rfloor$, and from inequality (10) we obtain $d/q^l - 1 < r \leq d/q^l$, namely $r = \lfloor d/q^l \rfloor$.

Corollary 4 (Bound A). *Let $l = \lfloor \log_q d \rfloor$ and $r = \lfloor d/q^l \rfloor$. Then*

$$S_q(k,d) \geq d + \sum_{i=1}^{k-1} \left\lceil \frac{q^l r}{q^i} \right\rceil.$$

Next we generalize Proposition 2.

Proposition 4. *Let q, k and d be fixed, and let l be the maximum integer such that q^l divides d. Then*

$$N_q(q^k, d) \geq \sum_{i=0}^{h} \left\lceil \frac{d}{q^i} \right\rceil,$$

where h is the minimum between $k-1$ and l.

Corollary 5 (Bound B). *Let q, M and d be fixed, let k be the maximum integer such that $q^k \leq M$, and let l be the maximum integer such that q^l divides d. Then*

$$N_q(M, d) \geq \sum_{i=0}^{h} \left\lceil \frac{d}{q^i} \right\rceil,$$

where h is the minimum between $k-1$ and l.

We consider now the following bounds, which can be seen as weaker versions of the Griesmer bound or as an extension of the Plotkin bound.

Proposition 5. *For each choice of q, k and d, we have*

$$N_q(q^k, d) \geq \left\lceil \sum_{i=0}^{k-1} \frac{d}{q^i} \right\rceil = \left\lceil d \left(\frac{1 - \frac{1}{q^k}}{1 - \frac{1}{q}} \right) \right\rceil.$$

Observe that if the code has a number of words $M \geq q^k$, then by removing $M - q^k$ codewords we obtain an $(n, q^k, d)_q$-code and we can apply Proposition 5. We obtain the following Corollary.

Corollary 6 (Bound C). *For each choice of q, k and d,*

$$N_q(M, d) \geq \left\lceil d \left(\frac{1 - \frac{1}{q^k}}{1 - \frac{1}{q}} \right) \right\rceil . \tag{11}$$

where k is the larger integer such that $M \geq q^k$.

5 Counterexamples to the Griesmer bound

In this section we provide a binary systematic (nonlinear) code for which the Griesmer bound does not hold. It has been known that there exist pairs (k, d) for which $N_2(2^k, d) < g_2(k, d)$, but it has not so far been clear whether the same is true for systematic codes or not. We consider a nonlinear non-systematic code whose length contradicts the Griesmer bound. Then we make use of this code to construct a systematic code contradicting the Griesmer bound. In [Lev64], Levenshtein has shown that if Hadamard matrices of certain orders exist, then the binary codes obtained from them meet the Plotkin Bound. Levenshtein's method to construct such codes can be found also in the proof of Theorem 8, of [MS77, Ch. 3,§2].

We can construct a $(19, 16, 10)_2$-nonlinear and non-systematic code C, obtained using Levensthein's method, as explained in [MS77, Ch. 3,§2]. For details, see [BGMS15]. We consider the cyclic code C_l of length 15 associated to the complete defining set $S = \{0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12\}$, which is a code with 16 codewords and distance 8. We obtain a new code $\bar{C}$ by concatenating each codeword in C_l with a different codeword in C. In this way $\bar{C}$ is an $(34, 16, 18)_2$-systematic code. Since $g_2(4, 18) = 35$, $S_2(4, 18) < g_2(4, 18)$, proving that the Griesmer bound is in general not true for systematic codes (for details, see [BGMS15]).

6 Aknowledgements

The authors would like to thank Eleonora Guerrini and Massimiliano Sala. The authors would also like to thank the anonymous reviewer for interesting comments.

References

AB08. T. L. Alderson and A. A. Bruen, *Maximal AMDS codes*, Applicable Algebra in Engineering, Communication and Computing **19** (2008), no. 2, 87–98.

AG09. T. L. Alderson and A. Gács, *On the maximality of linear codes*, Designs, Codes and Cryptography **53** (2009), no. 1, 59–68.

BGMS15. E. Bellini, E. Guerrini, A. Meneghetti, and M. Sala, *On the Griesmer bound for nonlinear codes*, arXiv.org (2015).

BGS14. E. Bellini, E. Guerrini, and M. Sala, *Some bounds on the size of codes*, IEEE Trans. Inform. Theory **60** (2014), no. 3, 1475–1480.

Del73. P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. (1973), no. 10, vi+97.

Gri60. J. H. Griesmer, *A bound for error-correcting codes*, IBM Journal of Research and Development **4** (1960), no. 5, 532–542.

Hil86. R. Hill, *A first course in coding theory*, Clarendon Press Oxford, 1986.

HP03. W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

Joh71. S. Johnson, *On upper bounds for unrestricted binary-error-correcting codes*, Information Theory, IEEE Transactions on **17** (1971), no. 4, 466–478.

Kle04. A. Klein, *On codes meeting the Griesmer bound*, Discrete Mathematics **274** (2004), no. 1–3, 289–297.

Lev64. V. I. Levenshtein, *The application of Hadamard matrices to a problem in coding*, Problems of Cybernetics (1964), no. 5, 166–184.

Mar97. T. Maruta, *On the Achievement of the Griesmer Bound*, Designs, Codes and Cryptography **12** (1997), no. 1, 83–87.

MS77. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I and II*, North-Holland Publishing Co., Amsterdam, 1977.

Plo60. M. Plotkin, *Binary codes with specified minimum distance*, Information Theory, IRE Transactions on **6** (1960), no. 4, 445–450.

SS65. G. Solomon and J. J. Stiffler, *Algebraically punctured cyclic codes*, Information and Control **8** (1965), no. 2, 170–179.

Van80. H. Van Tilborg, *On the uniqueness resp. nonexistence of certain codes meeting the Griesmer bound*, Information and control **44** (1980), no. 1, 16–35.