

On codes meeting the Griesmer bound

Andreas Klein

March 20, 2003

Abstract

We investigate codes meeting the Griesmer bound. The main theorem of this article is the generalization of the nonexistence theorem of [7] to a larger class of codes.

keywords: Griesmer bound, extending codes, nonexistence theorem, code construction

1 Introduction

We only consider linear codes over a finite field \mathbb{F}_q . A central problem of coding theory is to determine the minimum value of $n = n_q(k, d)$, for which an $[n, k, d]_q$ code exists. A well known lower bound for $n_q(k, d)$ is:

Theorem 1 (Griesmer bound, see [1] for $q = 2$ and [8] for $q > 2$)

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

It is a natural question for which values of k, d, q we can achieve equality.

We know that the Griesmer bound is not sharp for the following values of k, d, q :

Theorem 2 (see [6],[7])

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 for $q \geq 2k-3$, $k \geq 6$.

That the value of d in Theorem 2 is the largest value of d such that no $[g_q(k, d), k, d]_q$ code exists, follows from:

Theorem 3 (see [4])

Let $s = \lceil d/q^k - 1 \rceil$, $k > u_1 \geq u_2 \geq \dots \geq u_p$ with $u_i > u_{i+q-1}$. Then $n_q(k, d) = g_q(k, d)$ if $d = sq^{k-1} - \sum_{i=1}^p q^{u_i-1}$ and if $\sum_{i=1}^{\min(s+1,p)} u_i \leq sk$.

Prominent examples of codes meeting the Griesmer bound are the simplex code and the $[11, 6, 5]_3$ Golay code. Many authors have investigated classes of codes meeting the Griesmer bound (see for example [3],[9]). Finite projective geometries play an important role in the study of these codes. For example in [2] minihypers are used to characterise codes meeting the Griesmer bound.

In this paper we prove by shortening and extending codes, that for certain pairs d and d' the existence of a $[g_q(k, d), k, d]_q$ code is equivalent to the existence of a $[g_q(k, d'), k, d']_q$ code. Especially we will use this method to extend the nonexistence theorem 2 to a greater class of codes.

2 Preliminaries

In this section we give a geometric description of a code. We will always assume $k \geq 3$. The description uses the projective space $PG(k-1, q)$. By θ_i we denote the number of points in a subspace of dimension i , i.e. $\theta_i = \frac{q^{i+1}-1}{q-1}$.

Let C be a code which does not have any coordinate position in which all codewords have a zero entry. The columns of a generator matrix of C can be considered as a multiset M of n points in $PG(k-1, q)$.

An i -point is a point that has multiplicity i . For each subset S of $PG(k-1, q)$ denote the number of points of M in S by $c(S)$. Let

$$\gamma_i = \max\{c(S) \mid S \text{ is a subspace of dimension } i\}$$

Especially is γ_0 the maximum number i for which an i -point exists.

In this description many properties of the code can be easily recognized. For example $d = n - \gamma_{k-2}$ (see [4]).

In the sequel we will need upper bounds for γ_i . The following lemma will provide them:

Lemma 4 (see [5])

For $0 \leq j \leq k-3$,

$$\gamma_i \leq \gamma_{i+1} - \frac{n - \gamma_{i+1}}{\theta_{k-i-2} - 1}$$

holds.

Proof

Let S be a subspace of dimension i , which contains γ_i points. Counting the number of points in all $i+1$ dimensional subspaces that contain S we get:

$$n \leq (\gamma_{i+1} - \gamma_i)\theta_{k-i-2} + \gamma_i$$

An easy transformation of this inequality yields the assertion. □

In many cases we can use Lemma 4 to determine the exact value of γ_i . The simplest case is the determination of γ_0 :

Lemma 5 (see [7])

Let C be an $[n, k, d]_q$ code meeting the Griesmer bound.

If $(s-1)q^{k-1} < d \leq sq^{k-1}$ for a positive integer s , then $\gamma_0 = s$.

Proof

Since $g_q(k, d) > (s-1)\theta_k - 1$, we conclude $\gamma_0 \geq s$. Assume $\gamma_0 > s$. In this case we can assume with out loss of generality that the first $s+1$ columns of the generator matrix have the form $(1, 0, 0, \dots, 0)$. Deleting the fist row of the generator matrix we obtain an $[n-s-1, k-1, d]_q$ code. A contradiction, since $n-s-1 < g_q(k-1, d)$. \square

The next lemma will play an important role in the remaining part of the paper.

Lemma 6

Let $s+t < q$ and $d < d' = sq^{k-1} - (s+t)q^{k-2}$. If $\delta = g_q(k, d') - g_q(k, d) \leq \theta_{k-2}$, then

$$\gamma_i = sq^i - t\theta_{i-1} - \left\lfloor \frac{\delta}{q^{k-i-1}} \right\rfloor$$

for $1 \leq i \leq k-2$.

Proof

Lemma 4 yields $\gamma_i \leq sq^i - t\theta_{i-1} - \left\lfloor \frac{\delta}{q^{k-i-1}} \right\rfloor$ and by Lemma 5 we obtain $\gamma_0 = s$.

We will prove the lemma by induction.

Choose a subspace S of dimension i that contains exactly

$$\gamma_i = sq^i - t\theta_{i-1} - \left\lfloor \frac{\delta}{q^{k-i-1}} \right\rfloor$$

points. Since $n > \theta_{k-2-i}(sq^{i+1} - t\theta_i - \left\lfloor \frac{\delta}{q^{k-i}} \right\rfloor - \gamma_i - 1) + \gamma_i$, at least one $i+1$ dimensional subspace containing S contains at least $q^{i+1} - t\theta_i - \left\lfloor \frac{\delta}{q^{k-i}} \right\rfloor$ points. \square

3 Puncturing codes

We can construct an $[n-1, k, d-1]_q$ code from an $[n, k, d]_q$ code by deleting a column in its generator matrix. In many cases this new code is still optimal.

We call a code, that can be obtained by deleting columns in the generator matrix of C , a punctured code of C .

Theorem 7

If $d-1 \pmod{q^{l+1}} \geq q^l$ and $sq^{k-1} - sq^{k-1-l} < d < sq^{k-1}$, then each $[g_q(k, d), k, d]_q$ code contains a $[g_q(k, d - q^l), k, d - q^l]_q$ punctured code.

Proof

Since $d-1 \pmod{q^{l+1}} \geq q^l$, we obtain $g_q(k, d - q^l) = g_q(k, d) - \theta_l$.

By Lemma 5 we obtain $\gamma_0 = s$. Since $s(\theta_{k-1} - \theta_{k-1-l}) < n$, there exists a subspace of dimension l which contains no 0-point. If we decrease the multiplicity of each point in this subspace by one, we obtain a $[g_q(k, d - q^l), k, d - q^l]_q$ code. \square

4 Extending codes

In the preceding section we constructed new codes by deleting columns in the generator matrix. In this section we will investigate the reverse problem, i.e. we want to construct a $[g_q(k, d), k, d]_q$ code from a $[g_q(k, d - 1), k, d - 1]_q$ by adding a column in the generator matrix.

Our first result in this direction is:

Theorem 8

Let $s + t < q$ and $d = sq^3 - (s + t)q^2 - 1$. An $[n, 4, d]_q$ code meeting the Griesmer bound can be extended to an $[n + 1, 4, d + 1]_q$ code.

Proof

We have $n = sq^3 - t(q^2 + q + 1) - 1$. By Lemma 6 we conclude $\gamma_0 = s$, $\gamma_1 = sq - t$ and $\gamma_2 = sq^2 - t(q + 1)$. Since $(q^2 + q + 1)(\gamma_1 - s) + s = sq^3 - (q^2 + q + 1)$ for each s -point exactly one line through this point contains $\gamma_1 - 1 = sq - t - 1$ points, while all other lines contain γ_1 points. We say the line with $\gamma_1 - 1$ points is small.

Now we prove that all small lines have a point Q in common. Let P_1 and P_2 be two s -points. Let l_i denote the small line through P_i ($i = 1, 2$). The plane through l_1 and P_2 contains exactly $\gamma_2 - 1$ points (count the points on all lines through P_1). Therefore it is impossible that all lines through P_2 in that plane contain γ_1 points. Thus l_2 must intersect l_1 at a point Q . Let P_3 be an s -point that lies not in the plane P_1P_2Q . (Since $(s - 1)q + s = sq + (s - q) < \gamma_1$ all lines through P_1 contain at least one more s -point.) The small line l_3 through P_3 must intersect with l_1 and l_2 . Since P_3 does not lie in the plane P_1P_2Q , we conclude that Q lies on l_3 . Since no s -point lies in all three planes P_1P_2Q , P_1P_3Q and P_2P_3Q , we obtain that every small line must contain Q , since it must intersect with l_1 , l_2 and l_3 .

We add the point Q to the code. Since Q lies only on small lines, after the extension the equations $\gamma_0 = s$, $\gamma_1 = sq - t$ and $\gamma_2 = sq^2 - t(q + 1)$ are still satisfied. Thus the new code has the minimal distance $n + 1 - \gamma_2 = d + 1$. \square

With a recursion argument we can extend the result of Theorem 8 to codes of dimension $k > 4$.

Theorem 9

Let be $q > s + t$ 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 $d' = sq^{k-1} - (s + t)q^{k-2}$.

Proof

We will prove the proposition by induction over k . Theorem 8 proves the case $k = 4$. Now we assume $k > 4$.

Let $\delta = g_q(k, d') - g_q(k, d)$, since $d' - d \leq q^{k-4}$ we obtain $\delta \leq \theta_{k-4}$.

As in the proof of Theorem 8 we call a line through an s -point that contains less than $sq - t$ points small. The defect of the line is the difference to $sq - t$ points. The cumulative defect of all small lines through an s -point is $\delta \leq \theta_{k-4}$.

We are going to prove that there exist δ points, such that all small lines contains at least one of these points. By adding these points we obtain a $[g_q(k, d'), k, d']_q$ code.

First we assume that at least one small line has the defect 1. Let l be such a line and P be an s -point on l . Since

$$\theta_{k-2}(sq^{k-2} - t\theta_{k-3} - \theta_{k-5} - (sq - t) - 1) < (n - (sq - t))\theta_{k-3}$$

there must be a hyperplane h through l that contains at least $sq^{k-2} - t\theta_{k-3} - \theta_{k-5}$ points.

By induction hypothesis we find a point Q on l , such that all lines through an s -point of h and Q are small. Since all lines with $sq - t$ points contain at least two s -points, the number of small lines in h through Q is at least $\theta_{k-4} + 1$. Let P be an s -point not in h . The maximal δ small lines through P must intersect all small lines through Q . This is only possible if Q lies on a small line through P . This proves that Q lies only on small lines, thus we can add Q to our code. We repeat this argument until we have added δ points (and therefore there are no more small lines) or until all small lines have a defect > 1 .

Now we assume that all small lines have a defect $\geq f > 1$. Let l be a small line with defect f . Analogical to the previous case we can find a hyperplane h through l that contains at least $q^{k-2} - t\theta_{k-3} - f\theta_{k-5}$ points. Since all lines have a defect $\geq f$, we can transfer all previous arguments (including Theorem 8) and conclude that there must be a point Q in h , such that each line in h through Q is small. As in the previous case we conclude that all lines through Q are small. Since all small lines have a defect of at least f , we can add Q f -times. We repeat this process until there are no more small lines.

The code reached by this extension process still satisfies $\gamma_1 = sq - t$ and therefore $\gamma_i = (sq - t - s)\theta_{i-1} + s = sq^i - t\theta_{i-1}$. This is a $[g_q(k, d'), k, d']_q$ code with $d' = sq^{k-1} - (s + t)q^{k-2}$. \square

Remark:

It may be surprising that it is in general impossible to extend a $[g_q(k, d), k, d]_q$ code with

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

to a $[g_q(k, d'), k, d']_q$ code with

$$d < d' < sq^{k-1} - (s + t)q^{k-2} \quad .$$

Example:

Let $q = \bar{q}^2$ and C a $[g_q(k, d), k, d]_q$ code with $d = sq^{k-1} - (s + t)q^{k-2}$. We

remove all points from a Baer-subplane and obtain a $[g_q(k, d'), k, d']_q$ code with $d' = d - q - \sqrt{q} - 1$. This code can not be extended to a $[g_q(k, d' + 1), k, d' + 1]_q$ code, because each point lies on a line with γ_1 points.

If $s + t$ is small in comparison to q , we can improve the results in the theorems 8 and 9.

Theorem 10

Let $(s + t)^2 + 3(s + t) + 1 \leq q$ and $d = sq^2 - (s + t)q - 1$. Each $[n, 3, d]_q$ code meeting the Griesmer bound can be extended to an $[n + 1, 3, d + 1]_q$ code.

Proof

We have $n = sq^2 - t(q + 1) - 1$. By Lemma 6 we obtain $\gamma_0 = s$ and $\gamma_1 = sq - t$.

Since $(q + 1)(\gamma_1 - s) + s = sq^2 - t(q + 1)$ each s -point lies at exactly one line with $\gamma_1 - 1 = sq - t - 1$ points. All other lines through an s -point contain exactly γ_1 points. We call the lines with $\gamma_1 - 1$ points small.

As in Theorem 8 we are going to prove that all small lines have a point Q in common. Adding this point we obtain an $[n + 1, 3, d + 1]_q$ code.

Since $sq - 1 = (s - 1)(s + t) + s(q - s - t + 1)$ each line with γ_1 points must contain at least $q - s - t + 1$ points of multiplicity s . Therefore every line with $\gamma_1 - 1$ points contains at least $q - s - t$ points of multiplicity s .

We investigate a line l with γ_1 points. This line contains $q - s - t + 1$ points of multiplicity s . Therefore we have at least $q - s - t + 1$ different small lines. Let h be one of these small lines. Each other small line intersects h at a point of multiplicity less than s . Since h contains at most $s + t + 1$ points with such a multiplicity, we can find a point Q that lies on $\frac{q-s-t}{s+t+1}$ different small lines $\neq h$. Since $\frac{q-s-t}{s+t+1} \geq s + t + 1$ this point lies on at least $s + t + 2$ small lines (h and at least $s + t + 1$ other small lines).

Now we prove that all small lines go through Q . Assume that this is not true, i.e. there exists a small line k which does not meet Q . Each small line through Q intersects k at a point of multiplicity less than s . Since there are at least $s + t + 2$ small lines through Q , we conclude that at least $s + t + 2$ points of k have a multiplicity less than s . But k contains at least $q - s - t$ points of multiplicity s . This is a contradiction, because k contains only $q + 1$ points.

Therefore all small lines intersect at Q and we can extend the code by Q . \square

Before we are able to combine the recursion arguments of Theorem 9 with the result of Theorem 10, we must take a closer look at the special case $d = sq^{k-1} - (s + t)q^{k-2}$. In [7] the following lemma was proven for the special case $t = 1$:

Lemma 11

As in Theorem 10 let $(s + t)^2 + 3(s + t) + 1 \leq q$. Let C be a $[g_q(k, d), k, d]_q$ code with $d = sq^{k-1} - (s + t)q^{k-2}$. Let l be a line that contains an r -point, but no point of greater multiplicity.

Then l contains exactly $rq - t$ points.

Proof

In the case $r = s$ we have proven this in Lemma 6.

If P is an s -point, then all lines through P contain exactly $sq - t$ points. The plane π through P and l contains therefore $(q + 1)(sq - t - s) + s = sq^2 - t(q + 1)$ points. (There are no small lines.)

Each line different from l in π with intersect l at an r -point contains at least $[sq^2 - t(q + 1)] - r(q + 1) - (q - 1)(sq - t - r)$ points. (The plane π contains $sq^2 - t(q + 1)$ points, the line l contains at most $(q + 1)r$ points and each other line contains at most $sq - t$ points (Lemma 4).) Since

$$s + 2t + 2r - 1 < (s + t)^2 + 3(s + t) + 1 \leq q$$

the number of points on l is greater than $(s - 1)(q + 1)$. Thus the line contains an s -point and therefore exactly $sq - t$ points.

We look at all lines in π through a fixed r -point of l . Since all lines but l through this point contain exactly $sq - t$ points, we can easily calculate the number of points on l . l contain exactly $rq - t = [sq^2 - t(q + 1)] - q(sq - t - r)$ points. \square

Now we are able to combine the recursion method of Theorem 9 with the result of Theorem 10.

Theorem 12

If $(s + t)^2 + 3(s + t) + 1 \leq q$, than 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 $d' = sq^{k-1} - (s + t)q^{k-2}$.

Proof

The structure of the proof is the same as for the proof of Theorem 9. But this time we have to do more work to identify the candidates for the extension.

We only study the case that there exists a small line with defect 1. The case that all lines have a defect > 1 is analogical to the corresponding case in the proof of Theorem 9.

As in the proof of Theorem 9 we find a hyperplane h that contains at least $sq^{k-2} - t\theta_{k-3} - \theta_{k-4} + 1$ points.

By induction hypothesis we can find points in h which lie only on small lines. Adding these points we can extend h to a $[g_q(k - 1, d''), k - 1, d'']_q$ code with $d'' = sq^{k-2} - (s + t)q^{k-3}$.

Let P be a point in h which lies only on small lines. By Lemma 11 applied to the code after the extension we know that each line, that contains only points of multiplicity r , contains less than $rq - t$ points.

Let Q be an s -point not in h . Since by Lemma 11 no line with less than $rq - t$ points, can contain an r -point and lie in a plane with $sq^2 - t(q + 1)$ points, we conclude, that each line in h through P must intersect with a small line

through Q . Since only $\theta_{k-4} - 1$ lines through Q are small, this implies that PQ is a small line.

Thus all lines through P are small ones and we can add P to the code.

Adding as in the proof of Theorem 9 one point after another, we reach a $[g_q(k, d'), k, d']_q$ code with $d' = sq^{k-1} - (s+1)q^{k-2}$. \square

Together with Theorem 2 the Theorems 9 and 12 yields the following nonexistence theorem:

Corollary 13

There is no $[g_q(k, d), k, d]_q$ code, if $q \geq 2k - 3$, $k \geq 4$ and

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

Furthermore if $q \geq k^2 + k - 1$, than there exists no $[g_q(k, d), k, d]_q$ code with $k \geq 3$ and

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

Proof

By Theorem 9 and Theorem 12 we can extend these codes to a $[g_q(k, d'), k, d']_q$ code with $d' = (k-2)q^{k-1} - (k-1)q^{k-2}$. By Theorem 2 there is no such code. \square

5 Codes meeting the Griesmer bound

In the previous section we proved the nonexistence of codes, by extending them to known parameters. In this section we go in the opposite direction. We start with a known code (the s -fold repetition of the simplex code) and use it to construct new codes with larger minimal distance.

Theorem 14

The Griesmer bound is sharp for $sq^{k-1} \leq d \leq sq^{k-1} + q - k + 2$.

Proof

In the case $d = sq^{k-1}$ we obtain $n = s\theta_{k-1}$ and the code where every point is an s -point meets the Griesmer bound.

If $d = sq^{k-1} + x$ ($1 \leq x \leq q$) we obtain $n = s\theta_{k-1} + k - 1 + x$. Thus it is sufficient to describe a code with $d = sq^{k-1} + q - k + 1$. All other codes can be obtained by deleting coordinates.

If the points $(1, x, \dots, x^{k-1})$ ($x \in \mathbb{F}_q$) and $(0, \dots, 0, 1)$ have multiplicity $s+1$ and all other points have multiplicity s , then the code has the desired property, because:

Each set of k $(s+1)$ -points is linearly independent (Vandermonde's determinant), i.e. no hyperplane contains more than $k-1$ points of multiplicity $s+1$.

The minimal distance of the code is therefore

$$n - s\theta_{k-2} - (k-1) = sq^{k-1} + q - k + 2. \quad \square$$

6 Open Problems

I want to close this article with some open problems:

1. Is it possible to prove Theorem 10 without the condition $(s+t)^2 + 3(s+t) + 1 \leq q$?
2. What is the maximal number of coordinates by which we can extend a code? Especially what is the maximal δ for which we can extend each $[g_q(3, d-\delta), 3, d-\delta]_q$ code to an $[g_q(3, d), 3, d]_q$ code ($d = sq^2 - (s+t)q$)? Theorem 10 proves $\delta \geq 1$.

References

- [1] J. H. Griesmer. A bound for error correcting codes. *IBM J. Res. Develop.*, 4:532–542, 1960.
- [2] N. Hamada. A characterization of some $[n, k, d; q]$ -codes meeting the Griesmer bound using a minihyper in a finite projective geometry. *Discrete Math.*, 116:229–268, 1993.
- [3] T. Helleseth. Projective codes meeting the Griesmer bound. *Discrete Math.*, 106/107:265–271, 1992.
- [4] R. Hill. Optimal linear codes. In C. Mitchell, editor, *Proc. 2nd IMA Conf. on Cryptography and Coding*, pages 75–104, Oxford, 1992. Oxford University Press.
- [5] R. Hill and I. Landgev. On the nonexistence of some quaternary codes. Technical Report MCS-94-05, Salford University, 1994.
- [6] T. Maruta. On the nonexistence of linear codes of dimension four attaining the Griesmer bound. In *Proceedings of the International Workshop on Optimal Codes and Related Topics*, pages 117–120, Sozopol, Bulgaria, 1995.
- [7] T. Maruta. On the Achievement of the Griesmer Bound. *Designs, Codes and Cryptography*, 12:83–87, 1997.
- [8] G. Solomon and J. J. Stiffler. Algebraically punctured cyclic codes. *Inform. and Control*, 8:170–179, 1965.
- [9] F. Tamari. A construction of some $[n, k, d; q]$ -codes meeting the Griesmer bound. *Discrete Math.*, 116:269–287, 1993.