A Note on the Griesmer Bound

L. D. Baumert and R. J. McEliece
Communications Systems Research Section

Griesmer's lower bound for the word length n of a linear code of dimension k and minimum distance d is shown to be sharp for fixed k, when d is sufficiently large. For $k \leq 6$ and all d the minimum word length is determined.

I. Introduction

Denote by $n(k, d)$ the smallest integer n such that there exists an (n, k) binary linear code with minimum distance at least d. In 1960 Griesmer (Ref. 1) proved that

$$n(k, d) \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil \quad \text{(see footnote 1)} \qquad (1.1)$$

and showed that for certain values of k and d the inequality (1.1) was in fact an equality. In 1965 Solomon and Stiffler (Ref. 2) simplified Griesmer's proof of (1.1) and at the same time generalized it to linear codes over an arbitrary finite field $GF(q)$, where it takes the form[1]

$$n(k, d) \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil \qquad (1.2)$$

[1]Actually these bounds were obtained in the form

$$n(k, d) \geq \sum_{i=0}^{k-1} d_i$$

where $d_0 = d$ and

$$d_i = \lceil d_{i-1}/q \rceil$$

It is easy to see, however, that

$$d_i = \lceil d/q^i \rceil$$

More important, however, Solomon and Stiffler introduced the notion of "puncturing" a $(q^k - 1, k)$ maximal-length shift-register code and showed that for many more values of k and d equality holds in (1.2).

In this note we shall use the technique of puncturing to show that for fixed k, when d is sufficiently large the Griesmer bound (1.2) is sharp. That is, we will show that for each k there exists an integer $D(k)$ such that if $d \geq D(k)$, then

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

As a matter of fact we will only prove this for $q = 2$, the extension to general q being easy but notationally awkward.

We shall use the notation

$$g(k, d) = \sum_{i=0}^{k-1} \lceil d/2^i \rceil$$

in the rest of the paper.

II. The Theorem of Solomon-Stiffler

Let V_k denote a k-dimensional vector space over $GF(2)$. Let $S_1, S_2, \cdots, S_t$ be subspaces of V_k of dimensions $k_1, k_2, \cdots, k_t$ such that no element (except 0) of V_k is contained in more than h of the S_i's. Then Solomon and Stiffler showed that there exists an (n, k) binary linear code with minimum distance d, where

$$n = h(2^k - 1) - \sum_{i=1}^{t} (2^{k_i} - 1)$$

and

$$d \geqq h2^{k-1} - \sum_{i=1}^{t} 2^{k_i - 1} = d' \qquad \text{(see footnote 2)}$$

Furthermore if the k_i are *distinct*, $n = g(k, d')$ and so the code is length-optimal; i.e., $n(k, d) = g(k, d)$. Finally they showed that a sufficient condition for the existence of such subspaces S_i is that

$$\sum k_i \leqq kh$$

III. Main Result

THEOREM: *For each k there exists an integer $D(k)$ such that $n(k, d) = g(k, d)$ if $d \geqq D(k)$.*

Proof: We show that

$$D(k) = \left\lceil \frac{k-1}{2} \right\rceil 2^{k-1}$$

will do. Write

$$d = d_0 + (h-1)2^{k-1}$$

where $1 \leqq d_0 \leqq 2^{k-1}$. Then if

$$d \geqq \left\lceil \frac{k-1}{2} \right\rceil 2^{k-1}$$

it follows that

$$h \geqq \left\lceil \frac{k-1}{2} \right\rceil$$

Next we write $2^{k-1} - d_0$ in its binary expansion

$$2^{k-1} - d_0 = \sum_{i=1}^{t} 2^{k_i - 1} \qquad 0 < k_1 < k_2 < \cdots < k_t < k$$

[2]It can be shown that $d = d'$ unless the dual subspaces $S_i^{\perp}$ completely cover V_k.

Then

$$\sum_{i=1}^{t} k_i \leqq 1 + 2 + \cdots + k - 1 = k(k-1)/2 \leqq k \cdot h$$

and so by the results of Solomon-Stiffler quoted in *Section II*, $n(k, d) = g(k, d)$.

IV. Numerical Results:

We have been able to calculate the exact values of $n(k, d)$ for $k \leqq 6$ and all d. It turns out that the value

$$D(k) = \left\lceil \frac{k-1}{2} \right\rceil 2^{k-1}$$

given in our theorem is extremely conservative; for example for $k = 6$ our theorem only guarantees that if $d \geqq 96$, $n(6, d) = g(6, d)$, while $d \geqq 20$ would do. Much of this disparity arises from our use of the very weak sufficient condition

$$\sum k_i \leqq kh$$

for the existence of subspaces $S_1, S_2, \cdots, S_t$.

Thus consider the example $k = 6$, $d = 35$. Examining the proof in Section 3, we write $35 = 3 + 1 \cdot 32$ ($h = 2$), and $32 - 3 = 29 = 2^4 + 2^3 + 2^2 + 2^0$. Thus we need to find subspaces of V_6 dimensions 5, 4, 3, and 1 which cover each nonzero vector of V_6 at most twice. Since $5 + 4 + 3 + 1 = 13 > 6 \cdot 2$, the condition of Solomon-Stiffler does not apply. However, if the vectors of V_6 are coordinatized $x = (x_1, x_2, \cdots, x_6)$, consider the following subspaces:

$S_1 = \{x : x_1 = 0\}$	dimension 5
$S_2 = \{x : x_2 = x_3 = 0\}$	dimension 4
$S_3 = \{x : x_4 = x_5 = x_6 = 0\}$	dimension 3
$S_4 = \{111111 \text{ and } 000000\}$	dimension 1

These subspaces have the desired property of covering each nonzero vector at most twice, and so $n(6, 35) = g(6, 35)$.

However, even if we knew exact necessary and sufficient conditions for the existence of the subspaces S_i, we would not always get the best possible code. For $k = 6$, $d = 17$ we would need subspaces of dimensions 4, 3, 2, and 1 which covered every nonzero element at most once;

but it is easy to see that any two subspaces of dimensions 4 and 3 in V_6 must share at least one nonzero vector. Thus the Solomon-Stiffler results could not yield a (37, 6) code with $d = 17$. However in his original paper (Theorem 5) Griesmer gave a construction which yields such a code.

We conclude the paper with a table of those values of k and d with $k \leq 6$ for which $n(k, d) > g(k, d)$ (Table 1). The column labeled "comments" explains how we calculate $n(k, d)$. "HB" means that the Hamming bound forces $n(k, d) > g(k, d)$. "Search" means that a computer search found no codes of length $g(k, d)$. An entry like "$n(5, 3)$" refers to the bound, proved by Griesmer, that

$$n(k, d) \geqq d + n(k - 1, \lceil d/2 \rceil)$$

Thus if $n(k - 1, \lceil d/2 \rceil) > g(k - 1, \lceil d/2 \rceil)$, then $n(k, d) > g(k, d)$ as well. We only list odd d because of the relationship $n(k, d) = n(k, d + 1) - 1$ for odd d.

References

1. Griesmer, J. H., "A Bound for Error-Correcting Codes," *IBM J. Res. Develop.*, Vol. 4, pp. 532–542, 1960.
2. Solomon, G., and Stiffler, J. J., "Algebraically Punctured Cyclic Codes," *Inf. and Cont.*, Vol. 8, pp. 170–179, 1965.

Table 1. Values of k and d with $k \leq 6$ for which $n(k, d) > g(k, d)$

k	d	$g(k, d)$	$n(k, d)$	Comments
5	3	8	9	HB; (9, 5) = (15, 11) Hamming shortened
5	5	12	13	Search; (13, 5) = (15, 7) BCH shortened
6	3	9	10	HB; (10, 6) = (15, 11) Hamming shortened
6	5	13	14	n (5, 3); (14, 6) = (15, 7) BCH shortened
6	7	16	17	n (5, 4); (17, 6) = (23, 12) Golay shortened
6	9	21	22	n (5, 5); (22, 6) found *ad hoc*[a]
6	11	24	25	n (5, 6); (25, 6) found *ad hoc*[b]
6	13	28	29	Search; (29, 6) = (31, 6) RM minus 2 columns
6	19	40	41	Search; (41, 6) = S.-S. construction w. dims. 3, 3, 3, 1. ($h = 1$).

[a]Take as columns in the generator matrix the 6-place binary expansions of: 2, 3, 4, 6, 8, 9, 11, 12, 16, 17, 20, 21, 26, 32, 33, 38, 44, 51, 58, 61, 62, 63.

[b]Take as columns 1, 1, 2, 4, 6, 8, 10, 13, 16, 18, 21, 27, 28, 31, 32, 34, 37, 43, 45, 46, 53, 54, 57, 58, 60.