TABLE IV
EQUATIONS AND CONDITIONS USED TO PROVE (36)

| Case | Equation number | Condition |
|---|---|---|
| $j_3 < j_1 < j_2$ | (19-$\alpha$), (18-$\beta$) | $p_2 > 0$, $q_1 < 0$ |
| $j_3 < j_2 < j_1$ | (18-$\alpha$), (21-$\beta$) | $p_1 > 0$, $q_4 > 0$ |
| $j_1 < j_2 < j_3$ | (21-$\alpha$), (18-$\beta$) | $p_4 < 0$, $q_1 < 0$ |
| $j_2 < j_1 < j_3$ | (18-$\alpha$), (19-$\beta$) | $p_1 > 0$, $q_2 < 0$ |

and

$$j_{i_1} \equiv j_{i_2} + 1 \equiv j_{i_3} + 1 \equiv j_4 - 1 \qquad \bmod 3.$$

That is, it is known that these conditions are equivalent to those given by (II)-(iv), (II)-(v), and (II)-(vi) in Table I when $m_k = 3$. Thus the restriction on $j_{\max}(J)$ does not change.

Moreover the set of $a_i$ obtained from $a_{i_1} = (r-1)a_{i_2} = a_{i_3} = -(r-1)a_4$ also satisfies (37). Thus the situation as previously described may happen also for $A(r,2)$. However, we have from (38)

$$j_{i_1} + 1 \equiv j_{i_2} + 1 \equiv j_{i_3} \equiv j_4 \qquad \bmod 2,$$

which are equivalent to one of the congruences in (II)-(iv), (II)-(v), or (II)-(vi). Thus no new restriction on $j_{\max}(J)$ is needed here.

Except for the case of $a_{i_1} = (r-1)a_{i_2} = a_{i_3} = -(r-1)a_4$, we can find several sets of $a_i$ satisfying (37). However, we cannot find those sets of $a_i$ in Table I. This fact means that under those conditions $J$ cannot be divided by an $A$ that is composed of three or more $A(r,m_k)$, even if one of them is $A(r,2)$. Therefore this discussion does not impose any more stringent restriction on $j_{\max}(J)$.

*Case (III)*

*(III)-(ii):* This case has the same condition on $j_i$ as that considered by Kondratyev and Trofimov [1] for the binary case. It follows from the results obtained there that (13) is a sufficient condition for $A \nmid J$.

Finally we must consider the cases where $w_r(J) < 4$. However, the details for these cases are omitted here, because they can be discussed in a similar and even simpler way than that in the case of $w_r(J) = 4$. The result obtained is that looser restrictions than (5) and (13) will do.

From all that has been discussed previously and the inequalities

$$\min_{I_1,I_2} \left( \prod_{k \in I_1} m_k + \prod_{k \in I_2} m_k \right) < \prod_{k \in I} m_k - 2 < \prod_{k \in I} m_k - 1$$

we can conclude that the following theorem is valid.

*Theorem 2:* A radix-$r$ $AN$ code generated by $A = \prod_{k \in I} A(r,m_k)$ has distance not less than five under the three conditions stated in Theorem 1.

ACKNOWLEDGMENT

The authors appreciate useful discussions with Prof. N. Honda. They are also indebted to Prof. K. Ikegaya for his guidance and support during this research.

REFERENCES

[1] V. N. Kondratyev and N. N. Trofimov, "Error-correcting codes with a Peterson distance not less than five," *Eng. Cybern.*, no. 3, pp. 85–91, 1969.
[2] W. W. Peterson, *Error Correcting Codes.* New York: Wiley, 1961, ch. 13.
[3] T. R. N. Rao and A. K. Trehan, "Single-error-correcting nonbinary arithmetic codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 604–608, Sept. 1970.
[4] J. L. Massey, "Survey of residue coding for arithmetic errors," Int. Comput. Cent., UNESCO, Rome, Italy, Bull. 3, Oct. 1964, pp. 3–17.

## A Note on the Griesmer Bound

L. D. BAUMERT AND R. J. MCELIECE

***Abstract*—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 [1] proved that[1]

$$n(k,d) \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil \tag{1.1}$$

and showed that for certain values of $k$ and $d$ the inequality (1.1) was in fact an equality. In 1965 Solomon and Stiffler [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]

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

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 correspondence 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

Manuscript received April 10, 1972. This research was supported by the National Aeronautics and Space Administration under Contract NAS 7-100.
The authors are with the Jet Propulsion Laboratory, California Institute of Technology, Pasadena, Calif.

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

that no element (except 0) of $V_k$ is contained in more than $h$ of the $S_i$. Then Solomon and Stiffler showed that there exists an $(n,k)$ binary linear code with minimum distance $d$, where[2]

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

$$d \geq h2^{k-1} - \sum_{i=1}^{t} 2^{k_i-1} = d'.$$

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 $\sum k_i \leq kh$.

## III. Main Result

*Theorem:* For each $k$ there exists an integer $D(k)$ such that

$$n(k,d) = g(k,d), \qquad \text{if } d \geq D(k).$$

*Proof:* We show that $D(k) = \lceil (k-1)/2 \rceil 2^{k-1}$ will do. Write $d = d_0 + (h-1)2^{k-1}$, where $1 \leq d_0 \leq 2^{k-1}$. Then if $d \geq \lceil (k-1)/2 \rceil 2^{k-1}$ it follows that $h \geq \lceil (k-1)/2 \rceil$. Next we write $2^{k-1} - d_0$ in its binary expansion

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

Then

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

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 $k \leq 6$ and all $d$. It turns out that the value $D(k) = \lceil (k-1)/2 \rceil \cdot 2^{k-1}$ given in our theorem is extremely conservative; for example, for $k = 6$ our theorem only guarantees that if $d \geq 96$, $n(6,d) = g(6,d)$, while $d \geq 20$ would do. Much of this disparity arises from our use of the very weak sufficient condition $\sum k_i \leq kh$ 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 III, 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 $V_6$ of dimensions 5, 4, 3, and 1 that 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:

$$S_1 = \{x: x_1 = 0\} \qquad \text{dimension 5}$$

$$S_2 = \{x: x_2 = x_3 = 0\} \qquad \text{dimension 4}$$

$$S_3 = \{x: x_4 = x_5 = x_6 = 0\} \qquad \text{dimension 3}$$

$$S_4 = \{111111 \text{ and } 000000\} \qquad \text{dimension 1.}$$

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

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

TABLE I

| $k$ | $d$ | $g(k,d)$ | $n(k,d)$ | 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) = Solomon–Stiffler construction with dimensions 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.

need subspaces of dimensions 4, 3, 2, and 1 that 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 that yields such a code.

We conclude the paper with Table I, which shows those values of $k$ and $d$ with $k \leq 6$ for which $n(k,d) > g(k,d)$. The column titled "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 $n(k,d) \geq d + n(k-1, \lceil d/2 \rceil)$. 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] J. H. Griesmer, "A bound for error-correcting codes," *IBM J. Res. Develop.*, vol. 4, pp. 532–542, 1960.
[2] G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes," *Inform. Contr.*, vol. 8, pp. 170–179, 1965.

# A Note on One-Step Majority-Logic Decodable Codes

C. L. CHEN AND W. T. WARREN

***Abstract*—Construction of shortened geometric codes as shown here results in 1-step majority-logic decodable codes. The shortened codes retain the error-correction ability of the parent codes and the decoders for the shortened codes are much simpler than for the parent code. A table of shortened codes is given.**

## I. Shortened Finite Geometry Codes

A shortened cyclic code retains at least the error-correcting capability of the parent full-length cyclic $(n,k)$ code. In the case

Manuscript received April 17, 1972; revised July 5, 1972. This work was supported in part by the National Science Foundation under Grant GK-24879 and in part by the Joint Services Electronics program (U.S. Army, U.S. Navy and U.S. Air Force) under Contract DAAB-07-67-C-0199.
The authors are with the Coordinated Science Laboratory, University of Illinois at Urbana–Champaign, Urbana, Ill.