I. Introduction and Review of the Classical Griesmer Bound

The Griesmer bound is a classical technique (developed in 1960) for estimating the minimum length $n$ required for a binary linear code with a given dimension $k$ and minimum distance $d$. In this article, a unified derivation of the Griesmer bound and two new variations on it are presented. The first variation deals with linear codes which contain the all-ones vector; such codes are quite common and are useful in practice because of their "transparent" properties. The second variation deals with codes that are constrained to contain a word of weight $\geq M$. In both cases these constraints (the all-ones word or a word of high weight) can increase the minimum length of a code with given $k$ and $d$.

Lemma. Let $a = (a_1, \ldots, a_n)$ be a fixed binary vector of length $n$. If $b = (b_1, \ldots, b_n)$ is another binary vector of length $n$, let $b'$ be the vector obtained by puncturing $b$ at the positions where $a_i = 1$. Then

$$\text{wt}(b') = \frac{\text{wt}(b)}{2} + \frac{\text{wt}(a + b) - \text{wt}(a)}{2}$$

(1)

Proof: Without loss of generality, take $a = 0000000 1111111$ and $b = 0001111 1110000$.

$$a + b = 0001111 0001111$$

(2)

where $w = \text{wt}(a)$. Then, if $x = (x_1, x_2, \ldots, x_n)$ is any vector of length $n$, then $x' = (x_1, \ldots, x_{n-w})$. Similarly, define the complementary puncturing of $x$—at the components where $a_i = 0$ by $x'' = (x_{n-w+1}, \ldots, x_n)$, so that...
wt(\(x\)) = wt(\(x'\)) + wt(\(x''\)) for any vector \(x\). Applying this rule to the second and third line of Eq. (2) yields, noting that wt(\((a + b)'\)) = wt(\(b'\)) and wt(\((a + b)''\)) = wt(\(b''\)),

\[wt(b') + wt(b'') = wt(b)\]

\[wt(b') + [w - wt(b'')] = wt(a + b)\]

Adding these two equations, \(2wt(b') = wt(b) + wt(a + b) - wt(a)\), which is the same as Eq. (1).

In the rest of the article, the MacWilliams-Sloane ([6], Section 1.1) terminology of an \([n, k, d]\) code is used to describe a binary linear code with length \(n\), dimension \(k\), and minimum distance \(d\).

Theorem 1. Let \(C\) be an \([n, k, d]\) code, and let \(a\) be a codeword of weight \(d\). Let \(C'\) be the code obtained from \(C\) by puncturing each codeword at the coordinates where \(a_i = 1\). Then \(C'\) is an \([n-d, k-1, d']\) code with \(d' > \lceil d/2 \rceil\), and so its length must be > \(n(k-1, \lceil d/2 \rceil)\).

Proof: The code \(C'\) is by definition of length \(n-d\), since there are \(d\) punctured coordinates. To compute the dimension of \(C'\), use the fact that the puncturing mapping \(P\) from \(C\) to \(C'\) is a linear transformation, so that \(\text{rank}(P) + \text{nullity}(P) = \dim(C) = k\) ([4], Theorem 3.1.3). To find nullity(\(P\)), examine the set of codewords \(x \in C\) such that \(x' = 0\). If \(x'\) is such a codeword, then the 1's of \(x\) must be confined to the \(d\) coordinates where \(a\) is nonzero, so that either \(x = 0\) or \(wt(a + x) < d\). But since \(x + a\) is a codeword and \(d\) is the minimum weight of \(C\), it follows that \(x + a = 0\), i.e., \(x = a\). Thus, there are just two words in \(C\) that, when punctured, yield \(0\) and \(a\), and so nullity(\(P\)) = 1, so that \(\text{rank}(P)\), i.e., the dimension of \(C'\), is one less than the dimension of \(C\), i.e., \(k-1\). Finally, if \(b\) is an arbitrary codeword of \(C\) not equal to \(0\) or \(a\), \(wt(b + a) \geq d = wt(a)\), and so by the Lemma, \(wt(b') \geq \lfloor wt(b)/2 \rceil \geq \lceil d/2 \rceil\). Thus, every nonzero word in \(C'\) has weight \(\geq \lceil d/2 \rceil\).

Let \(n(k, d)\) be the minimum length of a binary code with Hamming distance \(\geq d\) and dimension \(k\). The original Griesmer bound can now be stated and proven ([3] or [6], p. 546).

Theorem 2 (Griesmer, 1960). If \(k \geq 2\), then

\[n(k, d) \geq d + n(k - 1, \lceil d/2 \rceil)\]

Proof: Let \(C\) be an \([n, k, d]\) binary linear code with \(n = n(k, d)\). Then the code \(C'\) described in Theorem 1 is an \([n - d, k - 1, d']\) code with \(d' \geq \lceil d/2 \rceil\), and so its length must be \(\geq n(k - 1, \lceil d/2 \rceil)\). Hence, \(n(k, d) - d \geq n(k - 1, \lceil d/2 \rceil)\).

Corollary 1 (Griesmer, 1960).

\[n(k, d) \geq d + [d/2] + [d/2^2] + \cdots + [d/2^{k-1}]\quad \text{for } k \geq 1\]

Proof: This follows from Theorem 2, combined with the self-evident result that \(n(1, d) = d\) for all \(d \geq 1\), with mathematical induction, and that \([\lfloor x/2 \rfloor] = \lfloor x/2 \rfloor\) (see [1] or [5], solution to exercise 1.2.4, p. 476).

II. The Griesmer Bound for Codes Containing the All-Ones Word

In many applications, it is necessary to consider codes that contain the all-ones vector, e.g., “transparent codes” for synchronizing phase-shift-keyed-modulated data ([2], Section 6.6.1), or for synthesizing good finite state-codes [7]. It is therefore useful and interesting to study the possible loss in performance induced by requiring a code to contain the all-ones vector. Thus let \(N(k, d)\) denote the minimum length of a binary code with Hamming distance \(\geq d\) and dimension \(k\) that contains the all-ones vector.

Theorem 3. If \(k \geq 2\), then (cf. Theorem 2).

\[N(k, d) \geq d + N(k - 1, \lceil d/2 \rceil)\]

Proof: Let \(C\) be an \([n, k, d]\) binary linear code containing the all-ones vector with \(n = N(k, d)\). Then the punctured code \(C'\) described in Theorem 2 is an \([n - d, k - 1, d']\) code that contains the all-ones vector (since puncturing an all-ones vector leaves another all-ones vector) with \(d' \geq \lceil d/2 \rceil\), and so its length must be \(\geq N(k - 1, d - 1)\). Hence, \(N(k, d) - d \geq N(k - 1, \lceil d/2 \rceil)\).

Theorem 4. Both \(N(1, d) = d\) and \(N(2, d) = 2d\) for all \(d \geq 1\).

Proof: For the \(k = 1\) result, take as the generator matrix

\[
G = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix}
\]

For the \(k = 2\) result, note that an \([n, 2, d]\) code with the all-ones vector has a \(2 \times n\) generator matrix of the form...
Denote by $n_0$ the number of columns of $G$ of the form \( \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix} \) and by $n_1$ the number of columns of the form \( \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 1 \end{pmatrix} \). Then, since the code has minimum weight $d$, it must follow that $n_1 \geq d$ and $n_0 \geq d$. Hence, $n = n_0 + n_1 \geq 2d$. On the other hand, by taking $n_0 = d$ and $n_1 = d$, one obtains a $[2d, 2, d]$ code containing the all-ones vector.

**Theorem 5.** If $k \geq 3$, then

\[
N(k, d) \geq d + \left\lfloor \frac{d}{2} \right\rfloor + \left\lfloor \frac{d}{2^2} \right\rfloor + \cdots + 2\left\lfloor \frac{d}{2^{k-2}} \right\rfloor
\]  

Proof: This follows by mathematical induction on $k$, using Theorem 3 as the boundary value and Theorem 4 as the induction step, again with the help of the result $\left\lfloor \frac{d}{2} \right\rfloor = \left\lfloor \frac{d}{2} \right\rfloor$ cited above.

**Examples.** Let $k = 3$ and $d = 3$. Then by the Corollary 1 and Theorem 5, $n(3, 3) \geq 3 + 2 + 1 = 6$ and $N(3, 3) \geq 3 + 2 + 2 = 7$. In both cases the bound is sharp, since there is a $[6, 3, 3]$ code, namely, a punctured $[7, 3, 4]$ simplex code with generator matrix

\[
G = \begin{pmatrix}
110100 \\
011010 \\
001101
\end{pmatrix}
\]

and a $[7, 3, 3]$ code with the all-ones word, namely,

\[
G = \begin{pmatrix}
111111 \\
100001 \\
010010
\end{pmatrix}
\]

Since $N(5, 9) \geq 9 + 5 + 3 + 2 \cdot 2 = 21$, there is no $[20, 5, 9]$ code with the all-ones word. There is, however, a $[21, 5, 9]$ code with the all-ones word, obtained from the $[16, 5, 8]$ biorthogonal code by repeating the information bits.

**Theorem 6.**

\[
N(k, 2) = \begin{cases} 
k + 1 & \text{if } k \text{ is odd} \\
k + 2 & \text{if } k \text{ is even}
\end{cases}
\]

**Proof:** Since there is plainly no $[k, k, 2]$ code, with or without the all-ones word, it follows that $N(k, 2) \geq k + 1$ for all $k$. The only $[k + 1, k, 2]$ code has the parity-check matrix

\[
H = \begin{pmatrix}
k + 1 & \cdots & 1 \\
1 & \cdots & 1
\end{pmatrix}
\]

This code contains the all-ones vector if and only if $k$ is odd, which proves that $N(k, 2) = k + 1$ if $k$ is odd, and $N(k, 2) \geq k + 2$ if $k$ is even. If $k$ is even, there is a $[k + 2, k, 2]$ code containing the all-ones word, with a parity-check matrix (illustrated for $k = 6$)

\[
H = \begin{pmatrix}
1111111 \\
11000000
\end{pmatrix}
\]

so that $N(k, 2) = k + 2$ when $k$ is even, as asserted.

**Corollary 2.**

\[
N(k, 3) \geq \begin{cases} 
k + 3 & \text{if } k \text{ is even} \\
k + 4 & \text{if } k \text{ is odd}
\end{cases}
\]

**Proof:** From Theorem 3, $N(k, 2) \geq 3 + N(k - 1, 2)$. The result now follows from Theorem 6.

**III. The Griesmer Bound for Codes Containing a Word of Bounded Weight**

As another variation on the Griesmer bound, let $N(k, d, M)$ denote the length of the shortest $[n, k, d]$ binary linear code that contains a word of weight $\geq M$.

**Theorem 7.**

\[
N(k, d, M) \geq d + N(k - 1, \lfloor d/2 \rfloor, \lfloor M/2 \rfloor)
\]

**Proof:** Let $C$ be an $[n, k, d]$ code containing a word of weight $\geq M$. As in the proof of Theorem 2, consider the code $C'$, which is an $[n - d, k - 1, d']$ code with $d' \geq \lfloor d/2 \rfloor$. Now let $b$ be a word of weight $\geq M$ in $C$. Then, by the Lemma, $\text{wt}(b') \geq \text{wt}(b)/2 \geq \lfloor M/2 \rfloor$. Thus, $C'$ is an $[n - d, k - 1, d']$ code with $d' \geq \lfloor d/2 \rfloor$ containing a word of weight $\geq \lfloor M/2 \rfloor$, i.e., $n - d \geq N(k - 1, \lfloor d/2 \rfloor, \lfloor M/2 \rfloor)$.
Theorem 8. If $M \geq d$ and $k \geq 2$,

$$N(k, d, M) \geq d + \left\lfloor \frac{d}{2} \right\rfloor + \left\lfloor \frac{d}{2^2} \right\rfloor + \cdots + \left\lfloor \frac{d}{2^{k-2}} \right\rfloor + \left\lfloor \frac{M}{2^{k-1}} \right\rfloor$$

Proof: This follows from Theorem 3 and the boundary value $N(1, d, M) = \max(M, d)$. □

Example. According to Theorem 5, $n(3,4) \geq 7$, and there is a $[7,3,4]$ code, i.e., the simplex code. However, this code has words only of weight 4. If one looks for a $[7,3,4]$ code with a word of weight 5 or more, an appeal to Theorem 8 shows that $N(3,4,5) \geq 4 + \left\lfloor \frac{4}{2} \right\rfloor + \left\lfloor \frac{5}{4} \right\rfloor = 8$. There is an $[8,3,4]$ code with a word of weight 6, namely, the code with generator matrix

$$G = \begin{pmatrix} 11111100 \\ 00011111 \\ 11001010 \end{pmatrix}$$

but it is unknown whether there is an $[8,3,4]$ code with a word of weight 5.

References


