$$\lambda_L = \left[\frac{1}{L}\right] \sum_{i=m-L+1}^{m} \prod_{i=j}^{m} X_i \tag{21}$$

where we have used the symbol λ_L rather than λ_m since the number of terms above depend only upon L. The conditioned expected values are then $\overline{\lambda_L}/N = 1$ and $\overline{\lambda_L}/C = (e^{Lr} - 1)/L(1 - e^{-r})$ while the corresponding variance when no change occurs is approximately $\overline{\lambda_L^2}/N \cong e^{Lr}/L^2(1 - e^{-r})$ where the approximation above is based upon the assumption $Lr \gg 1$.

If we set the detection threshold τ using an upper bound for the false alarm probability P_{FA} obtained by the Chebyshev inequality, we should use

$$\tau = \left[\frac{e^{Lr}}{L^2(1 - e^{-r})P_{FA}}\right]^{1/2} \tag{22}$$

If a target has emerged L or more samples in the past we can reasonably assume that the target will be detected if the average value of the test is well above threshold at the end of the processing of the L samples. We therefore seek the value of L for which $\lambda_L/C \gg \tau$. This requires

$$\frac{e^{Lr}}{L(1 - e^{-r})} \gg \frac{e^{Lr/2}}{L}\left[\frac{1}{(1 - e^{-r})P_{FA}}\right]^{1/2} \tag{23}$$

or

$$L \gg \frac{1}{r}[\log (1 - e^{-r}) - \log P_{FA}] \tag{24}$$

The term on the right is not very large. For example, if $r = 1$ and $P_{FA} = 10^{-7}$, $L \gg 21$. Hence, a relatively small number of past samples need be retained for detecting emerging targets with relatively high probability of detection.

Acknowledgment

In revising the manuscript, the authors gratefully acknowledge the comments and suggestions of one of the earlier reviewers.

References

[1] Marcus, M. B., and P. Swerling, Sequential detection in radar with multiple resolution elements, *IRE Trans. on Information Theory*, vol IT-8, Apr 1962, pp 237–245.
[2] Kendall, W., and I. S. Reed, A sequential test for radar detection of multiple targets, *IRE Trans. on Information Theory (Correspondence)*, vol IT-9, Jan 1963, p 51.
[3] Helstrom, C. W., A range-sampled sequential detection system, *IRE Trans. on Information Theory*, vol IT-8, Jan 1962, pp 43–47.
[4] Wainstein, L. A., and V. D. Zubakov, *Extraction of Signals from Noise*, Englewood Cliffs, N. J.: Prentice Hall, 1962, p 158.
[5] Middleton, D., *Statistical Communication Theory*, New York: McGraw-Hill, 1960, p 892.

On the Construction of Comma-Free Codes

WILLARD L. EASTMAN

Abstract—A construction is given which produces maximal (in number of words) comma-free codes for any odd word length n and any alphabet size σ.

I. Introduction

A FINITE CODE is called *synchronizable* if, and only if, there exists a least integer M such that the knowledge of the last M letters of any message suffices to determine a separation of code words. A block code $\mathcal{C}$ containing words of length n is called *comma-free* if, and only if, for any words $w = w_1w_2 \cdots w_n$ and $x = x_1x_2 \cdots x_n$ belonging to $\mathcal{C}$, the n letter overlaps

$$w_k \cdots w_nx_1 \cdots x_{k-1} \qquad (k = 2, \cdots, n)$$

are not words of the code. Comma-free codes form a subclass of synchronizable block codes for which M is less than $2n$. Golomb, Gordon, and Welch [1] have shown that the number of words of length n in a comma-free code constructed from an alphabet containing the letters $0, 1, \cdots, \sigma - 1$ cannot exceed

$$f(\sigma, n) = \frac{1}{n}\sum_{d|n} \mu(d)\sigma^{n/d}$$

where the summation is extended over all divisors d of n, and $\mu(d)$ is the Möbius function. Golomb, Gordon, and Welch conjectured that this bound is attainable for all odd values of n and all σ. However, Eastman and Even [2] have shown that $f(\sigma, n)$ is the maximum number of words that can be included in any synchronizable block code consisting of words of length n constructed from an alphabet of σ letters. Thus, if the conjecture holds, then for odd values of n no additional cost is incurred by imposing the comma-free constraint, although this is

Manuscript received April 24, 1964.
The author is with Sperry Rand Research Center, Sudbury, Mass.

much more restrictive than the synchronizability constraint.

The construction of comma-free codes has been discussed previously by Golomb and others [1], [3]–[5]. In [1], Golomb, Gordon, and Welch show how to construct maximal (in number of words) comma-free codes for $n = 3, 5, 7$, and 9. They further state that their methods can be extended to construct maximal comma-free codes for $n = 11, 13$, and 15. It should be noted, however, that lexicographic ordering does not give comma-free codes for these cases.

In the present paper a method is proposed for constructing comma-free codes $\mathcal{C}_{\sigma,n}$ for all odd values of n and all σ (see Definition 2 of Section II). In Section, III a proof is given of the comma-free property. In Section IV it is shown that the codes $\mathcal{C}_{\sigma,n}$ are maximal, and that the conjecture of Golomb, Gordon, and Welch is, in fact, true.

II. The Construction of Comma-Free Codes

The method of construction proposed in this section produces a maximal comma-free code for any given alphabet size σ and any odd word length n. In the discussion which follows, a *head* refers to any sequence of m letters ($1 \leq m < n$) at the beginning of a word, and a *tail* refers to any sequence of m letters ($1 \leq m < n$) at the end of a word. We begin our discussion with some examples, and introduce notation which will be useful in describing comma-free codes.

Example 1: $\sigma = 2, n = 3$

A comma-free code is given by the set of two words $\mathcal{C}_{2,3} = \{100, 101\}$, which we shall abbreviate as $\mathcal{C}_{2,3} = \{10a\}$.

The symbol a is always to be interpreted as replaceable by any letter of the alphabet $(0, 1, \cdots, \sigma - 1)$ which is not less than the predecessor of a in the code word. Thus

$$\{1010a\} = \{10100, 10101\}$$

and

$$\{10aaa\} = \{10000, 10001, 10011, 10111\}$$

Example 2: $\sigma = 2, n = 5$

$\mathcal{C}_{2,5} = \{1010a, 10aaa\}$. We shall abbreviate this further as $\mathcal{C}_{2,5} = \{10Ba\}$.

The symbol B is to be interpreted as replaceable both by the sequence 10 and by the sequence aa. (The substitution for B, of course, precedes the substitution for a.) Note that the sequence aa can never be replaced by 10. It follows that no even length tail of any word in $\mathcal{C}_{2,5}$ is a head of any word in $\mathcal{C}_{2,5}$. Hence, the code is comma-free.

Example 3: $\sigma = 2, n = 7$

$$\mathcal{C}_{2,7} = \{10BBa\}$$
$$= \{101010a, 1010aaa, 10aa10a, 10aaaaa\}$$

Each code defined thus far has been generated by a defining pattern consisting of a sequence $10 \cdots a$, where between the head 10 and the tail a there may occur a string of B's of length 0, 1, 2, $\cdots$. Let us now introduce further notation which substitutes for each sequence $10 \cdots a$ the number of B's contained in the sequence. Using this notation, and discarding the brackets, we say that

$\mathcal{C}_{2,3}$ is generated by the pattern 0

$\mathcal{C}_{2,5}$ is generated by the pattern 1

$\mathcal{C}_{2,7}$ is generated by the pattern 2

We turn now to the case of a general alphabet size σ. Every code which has been defined so far has contained only words beginning with the head 10. In the general case we shall consider for inclusion in $\mathcal{C}_{\sigma,n}$ only words beginning with a decreasing head xy, where $\sigma > x > y \geq 0$.

Example 4: $\sigma = \sigma, n = 3$

$\mathcal{C}_{\sigma,3} = \{xya\}$ is a comma-free code.

The symbol a again is to be interpreted as replaceable by any letter of the alphabet $(0, 1, \cdots, \sigma - 1)$ which is not less than the predecessor of a in the code word. Extending the concept of a defining pattern in the obvious way, we say that $\mathcal{C}_{\sigma,3}$ is generated by the defining pattern 0.

Example 5: $\sigma = \sigma, n = 5$

$$\mathcal{C}_{\sigma,5} = \{xyBa\} = \{xyxya, xyaaa\}$$

The symbol B is always to be interpreted as replaceable both by any decreasing sequence xy and by the sequence aa. Note that for any z the sequences generated by zx are distinct from the sequences generated by xy. It follows that the code $\mathcal{C}_{\sigma,5}$ is comma-free, for no even length tail of any word in the code is a head of any word in the code. Again, the code is said to be generated by the defining pattern 1. In a similar fashion, $\mathcal{C}_{\sigma,7}$ is generated by the pattern 2.

A maximal comma-free code can be obtained for the case $n = 11$ by selecting all words generated by the patterns 4 and 100 (i.e., $xyBaxyaxya$); for the case $n = 13$ by selecting all words generated by the patterns 5, 200 and 101. In [6] this approach is extended for defining maximal comma-free codes for all prime word lengths n not exceeding 31. It will not be used here, since it cannot be generalized for all odd n.

If a word w is generated by a pattern[1] $p = p_1 p_2 \cdots p_i$ we shall say that w is composed of i sections. The jth section is that part of the word which has been generated by p_j, and is of the form $xyB \cdots Ba$, where the sequence of B's is of length p_j, and the entire section is of length

[1] We shall also use the notation $p = p_{i1}p_{i2} \cdots p_{ii}$ to represent a pattern of length i.

$2p_i + 3$. For each section j of a word w we define a base σ numerical value v_j by

$$v_j = w_k\sigma^m + w_{k+1}\sigma^{m-1} + \cdots + w_{k+m-1}\sigma + w_{k+m}$$

where $m = 2p_j + 2$, and w_k is the initial letter of section j. Henceforth, in defining a code $\mathcal{C}_{\sigma,n}$ we shall require that if w is to be a word in $\mathcal{C}_{\sigma,n}$ then v, the word consisting of the numerical values of the sections of w, must be a word in some previously defined code $\mathcal{C}_{\rho,i}$. The definition of the codes thus proceeds inductively on n.

Definition 1

A defining pattern $p = p_{i1}p_{i2}\cdots p_{ii}$ generates all words of the form

$$\underbrace{xyB\cdots Ba}_{p_{i1}}\underbrace{xyB\cdots Ba}_{p_{i2}}\cdots\underbrace{xyB\cdots Ba}_{p_{ii}}$$

where B is replaceable both by xy and by aa; $\sigma > x > y \geq 0$ for every sequence xy; and a is replaceable by any letter which is not less than the predecessor of a.

Definition 2

The code $\mathcal{C}_{\sigma,1}$ is the alphabet $\{0, 1, \cdots, \sigma - 1\}$. The code $\mathcal{C}_{\sigma,n}$ (n odd, $n \geq 3$) consists of all words w which are both 1) generated by any of the odd length defining patterns of the forms

$$p_{11}$$

$$p_{31}p_{32}p_{33}$$

$$p_{51}p_{52}p_{53}p_{54}p_{55}$$

$$\cdots\cdots\cdots\cdots$$

$$p_{l1}p_{l2}p_{l3}\cdots p_{ll}$$

satisfying

a) $\sum_{j=1}^{i} p_{ij} = (n - 3i)/2$

b) l is the largest odd integer i such that $3i \leq n$

and 2) have the property that the word $v = v_1v_2\cdots v_i$ formed from the numerical values of the sections of w is a word in the code $\mathcal{C}_{\rho,i}$ for some ρ.

The one-letter defining patterns p_{11} will be called primary defining patterns; all others will be called secondary patterns. Words generated by a primary pattern will be called primary words, and their heads and tails will be called primary heads and primary tails. Every non-negative integer k is a primary pattern for some odd n, namely, $n = 2k + 3$.

Given any n letter sequence $z = z_1z_2\cdots z_n$ (n odd), we can construct a pattern p which generates some cyclic permutation of z. Define a sequence $s = s(z)$ by

$$s_1 = 0 \quad \text{if} \quad z_1 \geq z_n$$
$$= 1 \quad \text{if} \quad z_1 < z_n$$

and

$$s_i = 0 \quad \text{if} \quad z_i \geq z_{i-1}$$
$$= 1 \quad \text{if} \quad z_i < z_{i-1}$$

for all $j = 2, \cdots, n$. Now, if $s_i = 1$, then z_i cannot be derived from the symbol a; whereas, if $s_i = 0$, then z_i cannot be derived from the symbol y. Therefore, if $s_i\cdots s_k$ is an even length run of 1's, then $z_i\cdots z_k$ can be derived only from a sequence of the form $xyxy\cdots xy$; while if $s_i\cdots s_k$ is an odd length run of 1's, then $z_{i-1}z_i\cdots z_k$ can be derived only from a sequence of the form $xyxy\cdots xy$. (In examining the sequence s for runs of 1's, s_1 is considered to follow s_n.) All remaining letters of z can be derived only from a. By writing the appropriate symbol x, y, or a underneath each $s_i (j = 1, \cdots, n)$, we obtain a sequence from which z can be derived. This sequence is separated into sections as follows. Begin a new section following every odd length run of the symbol a. Since n is odd, and the symbols x and y occur only together as a pair, this division must create an odd number of sections. (One section, of course, may begin in a tail and end in a head of the sequence.) A defining pattern is obtained by replacing each section j by a number $p_j = (\nu - 3)/2$, where ν is the number of letters in the section. We arbitrarily select as the first section the one which contains z_1.

Example:

$z = 3\ 0\ 1\ 2\ 0\ 1\ 2\ 3\ 0\ 3\ 1\ 2\ 4\ 3\ 3\ 0\ 3\ 1\ 3\ 2\ 0\ 1\ 2\ 0\ 1\ 2\ 3\ 3\ 2$

$s = 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1$

$x\ y\ a, x\ y\ a\ a\ x\ y\ x\ y\ a, x\ y\ x\ y\ x\ y\ a, x\ y\ a, x\ y\ a\ a\ a, x\ y$

$p = 1\ 3\ 2\ 0\ 1$

Clearly, one cyclic permutation of z is generated by the pattern p.

If w is a word in a code $\mathcal{C}_{\sigma,n}$, then w is generated by a unique pattern p, and the division of w into its sections is unique. Since a section of a word always begins with a positive integer, there is, for a given alphabet, a one-to-one correspondence between sections and their numerical values. Consequently, with each word w of a code $\mathcal{C}_{\sigma,n}$ is associated a unique sequence v of numerical values of the sections of w.

III. Proof of the Comma-Free Property

In this section it will be established by induction on n that the codes $\mathcal{C}_{\sigma,n}$ are comma-free for all alphabet sizes σ and all odd word lengths n. A necessary and sufficient condition for a code $\mathcal{C}$ to be comma-free is given by Lemma 1, which is essentially a restatement of the definition of a comma-free code given earlier. Following Lemma 1, we give three more lemmas leading to the main result of the section (Theorem 1).

Lemma 1

A block code $\mathcal{C}$ is comma-free if, and only if, for every pair of sequences s^1 and s^2 such that $w = s^1s^2$ is a word in $\mathcal{C}$, either s^1 is not a tail of any word in $\mathcal{C}$, or s^2 is not a head of any word in $\mathcal{C}$.

Lemma 2

No even length primary tail t of a word in a code $\mathcal{C}_{\sigma_0,n_0}$ is a head of any word in any code $\mathcal{C}_{\sigma,n}$.

Proof: t begins with an odd-length (strictly) decreasing sequence of letters. But all even-length heads begin with an even-length decreasing sequence of letters. Therefore, t is not a head of any word in any code $\mathcal{C}_{\sigma,n}$.

Q.E.D.

Lemma 3

No even length primary head h of a word in a code $\mathcal{C}_{\sigma_0,n_0}$, is a tail of any word in any code $\mathcal{C}_{\sigma,n}$.

Proof: h ends with an odd-length nondecreasing sequence of letters. But all even-length tails end with an even-length nondecreasing sequence of letters. Therefore, h is not a tail of any word in any code $\mathcal{C}_{\sigma,n}$.

Q.E.D.

Lemma 4

If $w = w_1w_2 \cdots w_n$ is a word in a code $\mathcal{C}_{\sigma_0,n}$ (n odd, ≥ 3), then, for any non-negative α and β, $w' = (w_1 + \alpha)w_2 \cdots w_{n-1}(w_n + \beta)$ is a word in the code $\mathcal{C}_{\sigma,n}$ for some σ.

Proof: by induction on n. Lemma 4 is trivially true for $n = 3$, and whenever w is generated by a primary pattern. Suppose it is true for all $n < N$. Let $w = w_1w_2 \cdots w_N$ be a word in $\mathcal{C}_{\sigma_0,N}$ generated by a secondary defining pattern, and let $w' = (w_1 + \alpha)w_2 \cdots w_{N-1}(w_N + \beta)$ for non-negative α, β. Choose any $\sigma_1 > \text{Max}\,[\sigma_0 - 1, w_1 + \alpha, w_N + \beta]$, and form the sequence $v' = v'_1v'_2 \cdots v'_i$ consisting of the base σ_1 numerical values of the sections of w'. Clearly, w is a word in the code $\mathcal{C}_{\sigma_1,N}$. Form the sequence v of (base σ_1) numerical values of the sections of w. By Definition 2, v is a word in the code $\mathcal{C}_{\rho,i}$ for some ρ. But v' satisfies $v'_1 \geq v_1, v'_2 = v_2, \cdots, v'_{i-1} = v_{i-1}, v'_i \geq v_i$. By the inductive hypothesis, v' is a word in a code $\mathcal{C}_{\rho,i}$ for some ρ. Therefore, w' is a word in $\mathcal{C}_{\sigma,N}$ for some σ, for all conditions of Definition 2 are satisfied. Therefore, Lemma 4 is true for all n.

Q.E.D.

Theorem 1

If $w = s^1s^2$ is a word in a code $\mathcal{C}_{\sigma_0,n_0}$, then either s^1 is not a tail of any word in any code $\mathcal{C}_{\sigma,n}$, or s^2 is not a head of any word in any code $\mathcal{C}_{\sigma,n}$.

Proof: by induction on n_0. The hypothesis does not apply when $n_0 = 1$. The theorem is true for $n_0 = 3$; for, by Lemma 2, no even-length tail of a word in $\mathcal{C}_{\sigma_0,3}$ is a head of any word in any code $\mathcal{C}_{\sigma,n}$; and, by Lemma 3, no even-length head of a word in $\mathcal{C}_{\sigma_0,3}$ is a tail of any word in any code $\mathcal{C}_{\sigma,n}$. Suppose now the theorem is true for all σ_0, and all odd values of $n_0 < N$. Let s^1 and s^2 be any pair of sequences such that $w = s^1s^2$ is a word in the code $\mathcal{C}_{\sigma_0,N}$. Then the following statements are true:

1) If s^2 is an even-length tail beginning in an odd section of w, then, by Lemma 2, s^2 is not a head of any word in any code $\mathcal{C}_{\sigma,n}$; for, s^2 has an even-length primary tail as its head.

2) If s^2 is an even-length tail beginning in an even section of w, and the first letter of s^2 is not the initial letter of the section, then, by Lemma 3, s^1 is not a tail of any word in any code $\mathcal{C}_{\sigma,n}$; for, s^1 has an even-length primary head as its tail.

3) If s^2 is an odd-length tail beginning in an even section of w, then, by Lemma 2, s^2 is not a head of any word in any code $\mathcal{C}_{\sigma,n}$; for, s^2 has an even-length primary tail as its head.

4) If s^2 is an odd-length tail beginning in an odd section of w, and the first letter of s^2 is not the initial letter of the section, then, by Lemma 3, s^1 is not a tail of any word in any code $\mathcal{C}_{\sigma,n}$; for, s^1 has an even-length primary head as its tail.

5) If s^2 is an even-length tail beginning with the initial letter of an even section of w, then either s^2 is not a head of any word in any code $\mathcal{C}_{\sigma,n}$, or else s^1 is not a tail of any word in any code $\mathcal{C}_{\sigma,n}$. For, suppose there exists a word w^1 in some code $\mathcal{C}_{\sigma_1,n_1}$, such that s^1 is a tail of w^1; and that there also exists a word w^2 in some code $\mathcal{C}_{\sigma_2,n_2}$ such that s^2 is a head of w^2. Let $\sigma_3 = \text{Max}\,(\sigma_0, \sigma_1, \sigma_2)$. Then $w \in \mathcal{C}_{\sigma_3,N}$, $w^1 \in \mathcal{C}_{\sigma_3,n_1}$, and $w^2 \in \mathcal{C}_{\sigma_3,n_2}$. Form the word $v = v_1v_2 \cdots v_i$ consisting of the (base σ_3) numerical values of the sections of w. By construction of $\mathcal{C}_{\sigma_3,N}$, v belongs to a code $\mathcal{C}_{\rho,i}$ for some ρ and some $i < N$. Let $t^1 = v_1v_2 \cdots v_k$ and $t^2 = v_{k+1}v_{k+2} \cdots v_i$ be the head and tail, respectively, of v which correspond to the head s^1 and tail s^2 of w. Then the word formed from the (base σ_3) numerical values of the sections of w^1 has the tail $u^1 = (v_1 + \alpha)v_2 \cdots v_k$ for some non-negative α, while the word formed from the (base σ_3) numerical values of the sections of w^2 has the head $u^2 = v_{k+1}v_{k+2} \cdots v_{i-1}(v_i + \beta)$ for some non-negative β. But by Lemma 4, the word $v' = (v_1 + \alpha)v_2 \cdots v_{i-1}(v_i + \beta) = u^1u^2$ is a word in a code $\mathcal{C}_{\rho,i}$ for some ρ. Since $i < N$, the inductive hypothesis implies that either u^2 is never a head of any word in any code $\mathcal{C}_{\sigma,n}$, or else u^1 is never a tail of any word in any code $\mathcal{C}_{\sigma,n}$, leading to a contradiction. Therefore, either s^2 is never a head of any word in any code $\mathcal{C}_{\sigma,n}$, or else s^1 is never a tail of any word in any code $\mathcal{C}_{\sigma,n}$.

6) If s^2 is an odd-length tail beginning with the initial letter of an odd section of w, then by the same argument either s^2 is not a head of any word in any code $\mathcal{C}_{\sigma,n}$, or else s^1 is not a tail of any word in any code $\mathcal{C}_{\sigma,n}$.

All possibilities for s^2 have been accounted for. Therefore, for any pair of sequences s^1 and s^2 such that $w = s$ is a word in the code $\mathcal{C}_{\sigma_0,N}$ (any σ_0), either s^1 is not a t

of any word in any code $\mathcal{C}_{\sigma,n}$, or else s^2 is not a head of any word in any code $\mathcal{C}_{\sigma,n}$. Therefore, by induction, the theorem is true for all σ_0 and all odd n_0.

Q.E.D.

Corollary: The codes $\mathcal{C}_{\sigma,n}$ are comma-free for all σ and all odd n.

IV. Maximality

In this section, it will be shown that the codes $\mathcal{C}_{\sigma,n}$ of Definition 2 are maximal (in number of words), and that the conjecture of Golomb, Gordon, and Welch in [1] is true.

Let G_n be the cyclic group of transformations on the words generated by α, where

$$w_1w_2 \cdots w_n \xrightarrow{\alpha} w_2w_3 \cdots w_nw_1$$

Thus, G_n is the group of transformations which rotate the word. We say that two words w_1 and w_2 are equivalent if, and only if, there exists a transformation in G_n which maps w_1 into w_2. An equivalence class can contain at most n members. If a class contains exactly n (distinct) words, then the class will be called nondegenerate; otherwise it it will be called degenerate. A comma-free code can never contain a word from a degenerate equivalence class, nor more than one word from any nondegenerate equivalence class. A sufficient condition for maximality of a code $\mathcal{C}_{\sigma,n}$, then, is that it contain some word from every nondegenerate equivalence class. If this can be shown for all codes $\mathcal{C}_{\sigma,n}$ of Definition 2, then the conjecture of Golomb, et al., is true, for $f(\sigma, n)$ is the number of nondegenerate equivalence classes, as shown in [1].

Theorem 2

For any σ and any odd n, the code $\mathcal{C}_{\sigma,n}$ contains some word from every nondegenerate equivalence class.

Proof: If $n = 1$, the theorem is true; for, each letter of the alphabet $\{0, 1, \cdots, \sigma - 1\}$ constitutes a nondegenerate equivalence class, and there are no other classes. Suppose, now, the theorem is true for all (odd) $n < N$. Let w be any word in any nondegenerate equivalence class of words of length N constructed from an alphabet of σ letters. Construct a pattern p which generates some cyclic permutation of w. Now, $p = p_1p_2 \cdots p_i$ for some odd i in the range $1 \leq i \leq N/3$, and p clearly satisfies conditions 1(a) and 1(b) of Definition 2. Divide w into the i sections generated by the i components of p, and calculate the numerical values $v_j (j = 1, \cdots, i)$. Since w belongs to a nondegenerate class, $v = v_1v_2 \cdots v_i$ belongs to a nondegenerate class of words of length $i < N$. For some ρ, the code $\mathcal{C}_{\rho,i}$ contains a cyclic permutation of v, by the inductive hypothesis. Therefore, some cyclic permutation of w is included in the code $\mathcal{C}_{\sigma,N}$. Therefore, by induction on n, the theorem is true for all σ and all odd n.

Q.E.D.

Corollary: The codes $\mathcal{C}_{\sigma,n}$ are maximal (in number of words) for all σ and all odd n, and contain $f(\sigma, n)$ words, proving the conjecture of Golomb, Gordon, and Welch.

Acknowledgment

The author wishes to thank Dr. Shimon Even for his helpful criticism of the manuscript.

References

[1] Golomb, S. W., B. Gordon, and L. R. Welch, Comma-free codes, *Can. J. Math.*, vol. 10, 1958, pp 202–209.
[2] Eastman, W. L., and S. Even, On synchronizable and *PSK*-synchronizable block codes, *IEEE Trans. on Information Theory*, vol IT-10, Oct 1964, pp 351–356.
[3] Golomb, S. W., L. R. Welch, and M. Delbrück, Construction and properties of comma-free codes, *Biol. Medd. Dan. Vid. Selsk.*, vol 23, 1958, pp 3–34.
[4] Golomb, S. W., Efficient coding for the desoxyribonucleic channel, *Mathematical Problems in the Biological Sciences*, Am. Math. Soc., Providence, Rhode Island, 1962, pp 87–100.
[5] Jiggs, B. H., Recent results in comma-free codes, *Can. J. Math.*, vol 15, 1963, pp 178–187.
[6] Eastman, W. L., Defining patterns for comma-free codes for small prime word lengths, Sperry Rand Research Center Research Memo. 64–4, Apr 1964.

The Convolution Inequality for Entropy Powers

NELSON M. BLACHMAN, SENIOR MEMBER, IEEE

***Abstract*—The entropy power of a band-limited random process is the power of white Gaussian noise having the same entropy rate. Shannon's convolution inequality for entropy power states that the entropy power of the sum of two independent random processes is at least the sum of their entropy powers. This paper presents an improved version of Stam's proof of this inequality, which is obtained by mathematical induction from the one-dimensional case.**

Manuscript received April 1, 1964; revised December 16, 1964.
The author is with Sylvania Electronic Defense Labs., Mountain View, Calif.

Introduction

ALTHOUGH it is generally difficult to determine the capacity C of a channel of bandwidth W which accepts signals of power S and adds to them statistically independent noise of power N, Shannon[1] has shown that

[1] See Shannon [1], Theorem 18, p 641.