5 1967

SC-R-67-1131

June 1967

Conf- 670902--1

MASTER

THE ALGEBRAIC THEORY OF THE TWO-SIDED CORRELATION FUNCTION FOR BINARY CODES

G. J. Simmons

CESTI PRICES

H.C. \$2.00, MN 65

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

SANDIA LABORATORIES

OPERATED FOR THE U. S. ATOMIC ENERGY COMMISSION BY SANDIA CORPORATION

ALBUQUERQUE, NEW MEXICO; LIVERMORE, CALIFORNIA

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

Reg

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Presented at: The IEEE 1967 International Symposium
on Information Theory held in Athens,
Greece, September 11-16, 1967.

Issued by Sandia Corporation,
a prime contractor to the
United States Atomic Energy Commission

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission:

A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or

B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report.

As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor, to the extent that such employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

THE ALGEBRAIC THEORY OF THE TWO-SIDED CORRELATION FUNCTION FOR BINARY CODES

G. J. Simmons
Sandia Laboratory, Albuquerque

Introduction

This paper investigates the two-sided correlation function (correlogram) which occurs as the output of the detector in the correlation detection of a binary code word in an unsynchronized code stream. The correlogram, $X * Y$, is an $n+m-1$ symbol sequence generated by comparing the m symbol output, X , of the receiver with a reference word Y of length n stored in the detector. The k -th symbol in the correlation function $C_k(X, Y)$ is commonly formed by the rule^{1,2}

$$C_k(X, Y) = \frac{A - D}{A + D}$$

where A is the number of symbol agreements between X and Y and D is the number of disagreements when X has been shifted to the right $k+1$ symbol positions with respect to the leftmost symbol of Y . This operation is easily visualized as

$$\begin{array}{ccccccc} & & y_0 & & y_1 & \cdots & y_k & \cdots & y_{n-1} \\ & & & & & & & & \\ x_0 & x_1 & \cdots & x_{m-k-1} & x_{m-k} & \cdots & x_{m-1} & & \end{array}$$

where k assumes all values between 0 and $n+m-2$ inclusive.

For convenience in algebraic operations and to avoid repeated normalizations,^Δ throughout this paper it is assumed that

$$(X * Y)_k = (R + 1)C_k(X, Y) = A - D \quad (1)$$

^ΔThese restrictions do not affect the generality of the analysis since an appropriate linear transformation would convert the results to any other equivalent system.

and that the code symbols are ± 1 . The correlogram $X * Y$ can be represented simply, using these restrictions,

$$(X * Y)_k = \sum_{\ell=0}^R y_{\ell} x_{m-k+\ell-1} \quad (2)$$

where

$$R = \min[n-1, m-1, m+n-k-2, k]$$

and

$$X * Y = \sum_{k=0}^{m+n-2} (X * Y)_k 10^{m+n-k-2} \quad (3)$$

The base 10, as it is used here, is a positional notation and implies that the summation in Eq. (2) is carried out with a radix greater than m or n so that no carries are generated. The algebraic structure based on $X * Y$ for binary codes is much richer than the folded or cyclic correlation function ^{Δ} which has been widely discussed.^{2, 3}

Elementary Algebraic Properties of $*$

The proofs for most of the following statements are relegated to the appendices, since they are tedious and would interfere with the main development of the paper.

$$X * Y = \overleftarrow{X} Y \quad (4)$$

^{Δ} The cyclic correlation function $C(X, Y)$ is ordinarily computed only for cases in which $X = Y$:

$$mC_k(X, X) = (X * X)_k + (X * X)_{2m-k-2} = mC_{2m-k-2}(X, X)$$

This result, which is Theorem A of Appendix A, is referred to as the Product Rule, and says that the correlogram $X * Y$ is given by the arithmetic product of Y and X reversed, $\overleftarrow{X}$, carried out with a radix greater than m or n so that no carries are generated.

$$X * Y = X' * Y' \quad \text{Corollary A-1} \quad (5)$$

$$X * Y = \overleftarrow{Y * X} \quad \text{Corollary A-2} \quad (6)$$

$$X * Y = \overleftarrow{Y} * \overleftarrow{X} \quad \text{Corollary A-5} \quad (7)$$

Equations (6) and (7) show that the reversal operation $\leftarrow$ commutes with $*$, i.e.,

$$(*) (\leftarrow) = (\leftarrow) (*) \quad (8)$$

$$X * 1 = \overleftarrow{X} \quad \text{Corollary A-3} \quad (9)$$

$$X * -1 = \overleftarrow{X} \quad \text{Corollary A-3} \quad (10)$$

$$X * aY = aX * Y = a(X * Y) \quad \text{Corollary A-4} \quad (11)$$

where $a = \pm 1$. Equation (11) shows that the operator $*$ is homogeneous. Unfortunately $*$ is not a symmetric operator since

$$X * Y \neq Y * X \quad (12)$$

in general. A trivial (but adequate) proof that this is true may be drawn from Eqs. (4) and (9) from which it is seen that

$$X * 1 = \overleftarrow{X} \neq X = 1 * X$$

for any non-palindromic code X . Equation (11) can also be written in the form

$$X * Y' = X' * Y = -(X * Y) \quad (11')$$

The properties of * summarized in Eqs. (4) through (12) are adequate to show that an Abelian group G of four elements which operate on binary codes exists, whose elements are invariant under *. Let ℓ be the identity operator, ' code complementation, $\leftarrow$ code reversal, and $\leftarrow'$ code reversal followed by complementation; then the group multiplication table for G is given in Table 1.

	ℓ	'	$\leftarrow$	$\leftarrow'$
ℓ	ℓ	'	$\leftarrow$	$\leftarrow'$
'	'	ℓ	$\leftarrow'$	$\leftarrow$
$\leftarrow$	$\leftarrow$	$\leftarrow'$	ℓ	'
$\leftarrow'$	$\leftarrow'$	$\leftarrow$	'	ℓ

Table 1

Multiplication Table for G

It is obvious from Eqs. (5) and (7), by letting $X = Y$, that the following identities are valid:

$$\begin{aligned} X * X &= X' * X' \\ X * X &= \leftarrow X * \leftarrow X \\ X * X &= \leftarrow' X * \leftarrow' X \end{aligned} \quad (13)$$

Thus if

$$X = 1 \ 1 \ 1 \ -1 \ 1 \ -1 \ 1$$

so that

$$X * X = 1 \ 0 \ 1 \ -2 \ 3 \ -2 \ 7 \ -2 \ 3 \ -2 \ 1 \ 0 \ 1$$

then necessarily

$$\begin{aligned} X' &= -1 \ -1 \ -1 \ 1 \ -1 \ 1 \ -1 \\ \leftarrow X &= 1 \ -1 \ 1 \ -1 \ 1 \ 1 \ 1 \\ \leftarrow' X &= -1 \ 1 \ -1 \ 1 \ -1 \ -1 \ -1 \end{aligned}$$

LEGAL NOTICE

This report was prepared as an account of Government sponsored work. Neither the United States, nor the Commission, nor any person acting on behalf of the Commission: A. Makes any warranty or representation, expressed or implied, with respect to the accuracy, completeness, or usefulness of the information contained in this report, or that the use of any information, apparatus, method, or process disclosed in this report may not infringe privately owned rights; or B. Assumes any liabilities with respect to the use of, or for damages resulting from the use of any information, apparatus, method, or process disclosed in this report. As used in the above, "person acting on behalf of the Commission" includes any employee or contractor of the Commission, or employee of such contractor prepares, disseminates, or provides access to, any information pursuant to his employment or contract with the Commission, or his employment with such contractor.

all have the same correlogram. In this example X was chosen so that none of the codes were the same. It is possible to select X such that $X = \overleftarrow{X}$ (X palindromic) or so that $X = \overleftarrow{X}'$ (X anti-palindromic). In either case, precisely two distinct codes exist under G , since if $X = \overleftarrow{X}$ then $X' = \overleftarrow{X}$ and if $X = \overleftarrow{X}'$ then $X' = \overleftarrow{X}$ and $X \neq X'$ for all codes.

The number of palindromic code pairs X and X' of length m is

$$N_p = 2^{\left\lfloor \frac{m+1}{2} \right\rfloor - 1} \quad (14)$$

where $\left\lfloor \frac{m+1}{2} \right\rfloor$ denotes the integer part of the quotient. The first symbol in X determines a half set of codes of size 2^{n-1} since X' is in the complementary set. Half of the remaining symbol positions (if m is even) or half plus one (if m is odd) may be arbitrarily assigned. Equation (14) follows.

The number of anti-palindromic code pairs X and $\overleftarrow{X}'$ of length m is

$$N_{p'} = \begin{cases} 0 & \text{if } m = 2s + 1 \\ 2^{\frac{m-2}{2}} & \text{if } m = 2s \end{cases}$$

Equation (15) is justified by the same arguments used for Eq. (14). If m is odd the center symbol would have to equal its own complement, which is never true.

S , the total number of palindromic type codes, i. e., codes which have only two images under G , may be expressed simply as

$$S = N_p + N_{p'} = 2^s \quad (16)$$

where $m = 2s$ or $m = 2s + 1$.

If m is either a prime or twice a prime, Eq. (16) permits the direct calculation of the number of distinct auto-correlograms. The reasons for this restriction on m will be developed further later in the paper. The total

number of binary code words is 2^m . When $m = p$ or $2p$, S code words have only two images under G and the balance have four. In these cases, therefore, the number of distinct auto-correlograms is

$$N = 2^{m-2} + 2^{s-1}$$

or

$$N = 2^{m-2} + 2^{\left\lfloor \frac{m}{2} \right\rfloor - 1}$$

Table 2 tabulates N for $m < 25$ and $m = p$ or $2p$.

m	N
2	2
3	3
4	6
5	10
6	20
7	36
10	272
11	528
13	2,080
14	4,160
17	32,896
19	131,328
22	1,049,600
23	2,098,176

Table 2

Number of Distinct Auto-Correlograms for $m = p$ or $2p$

An important property of the operator $*$ is concerned with the question of when the code words commute, i. e.,

$$X * Y = Y * X \quad (18)$$

It was shown in Eq. (12) that $*$ is not a symmetric operator in general; however, there do exist code word pairs which satisfy Eq. (18). First observe, if Eq. (18) is to be satisfied, that by Eq. (6)

$$X * Y = Y * X = \overleftarrow{Y * X} = \overleftarrow{X * Y} \quad (19)$$

which shows that the correlogram is symmetric. Examples of this property are numerous:

$$(1 \ 1 \ -1 \ -1) * (1 \ 1 \ -1 \ 1 \ -1 \ -1) = (1 \ 1 \ -1 \ 1 \ -1 \ -1) * (1 \ 1 \ -1 \ -1) \\ = -1 \ -2 \ 1 \ 2 \ 0 \ 2 \ 1 \ -2 \ -1$$

$$(1 \ -1 \ 1) * (-1 \ 1 \ 1 \ -1) = (-1 \ 1 \ 1 \ -1) * (1 \ -1 \ 1) = -1 \ 2 \ -1 \ -1 \ 2 \ -1$$

Equations (8) and (19) permit the statement of Theorem 1.

Theorem 1:

If X and Y are invariant under one of the elements of G which commutes with $*$, then X and Y commute also.

Proof:

By Eqs. (5) and (8) all elements of G commute with the operator $*$, however, a code can be invariant only under $\overleftarrow{}$ and $\overleftarrow{}'$ since no code can be its own complement. Let $X = \overleftarrow{\overline{X}}$ and $Y = \overleftarrow{\overline{Y}}$, then

$$X * Y = \overleftarrow{\overline{X}} * \overleftarrow{\overline{Y}}$$

or by Eq. 7

$$X * Y = Y * X.$$

Let $X = \overleftarrow{\overline{X}}'$ and $Y = \overleftarrow{\overline{Y}}'$, then

$$X * Y = \overleftarrow{\overline{X}}' * \overleftarrow{\overline{Y}}'$$

or by Eq. 5

$$X * Y = \overleftarrow{\overline{X}}' * \overleftarrow{\overline{Y}}' = Y * X.$$

Symmetry Properties of *

Conditions sufficient for $X * Y = Y * X$ were proven in Theorem 1. In this section the argument developed there is extended to the general question of when is it possible for $X * Y = W * Z$ where the right and left hand factor codes are not equivalent under G , which has been shown to be a trivial case.

Let R_n be the Rademacher-Walsh matrix defined by,

$$R_n = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^n \quad (20)$$

where the exponent operation is to be the repeated Kronecker product. The rows of R_n are the Rademacher-Walsh functions. Define a transformation matrix T_n ,

$$T_n = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^n \quad (21)$$

which operates on R_n to form a matrix W_n ,

$$W_n = T_n R_n \quad (22)$$

For example if $n = 2$,

$$R_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad W_2 = \begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

The last row of W_2 is the first of R_2 reversed, the next to the last row of W_2 is the second row of R_2 reversed etc. This is true in general since

$$W_1 = T_1 R_1 = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

which is an interchange and reversal of the rows in R_1 . This construction makes it possible to state the following theorem.

Theorem 2

If R_n is the Rademacher-Walsh matrix as defined in Eq. (20) and W_n is R_n reflected about its minor diagonal, then the correlogram of any row of R_n and the corresponding row of W_n (symbolized by $\otimes$) is the same as for any other similarly chosen pair of rows in R_n and W_n and is given by

$$R_n \otimes W_n = (-1 \ 0 \ 1)^n$$

where the generalized Kronecker product is to be used on the right.

Example

$$R_2 \otimes W_2 = (-1 \ 0 \ 1)^2 = 1 \ 0 \ -1 \ 0 \ -1 \ 0 \ 1$$

and

$$R_3 \otimes W_3 = (-1 \ 0 \ 1)^3 = -1 \ 0 \ 1 \ 0 \ 1 \ 0 \ -1 \ 0 \ 1 \ 0 \ -1 \ 0 \ 1$$

Proof:

Theorem 2 is best proven by induction. By Eq. (20),

$$R_n = R_{n-1} \times \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and by Eq. (22)

$$W_n = W_{n-1} \times \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$$

Theorem 2 states that Eq. (23) is true. Assume Theorem (2) applies for some case, $n-1$, then:

$$(R_{n-1} \times (1 \ 1)) \otimes (W_{n-1} \times (-1 \ 1)) = (R_{n-1} \times (1 \ -1)) \otimes (W_{n-1} \times (1 \ 1)) \quad (23)$$

Theorem C can be applied to Eq. (23) to reduce it to the form:

$$(R_{n-1} \otimes W_{n-1}) \otimes 1 \ 1 * -1 \ 1 = (R_{n-1} \otimes W_{n-1}) \otimes 1 \ -1 * 1 \ 1$$

or

$$(R_{n-1} \otimes W_{n-1}) \otimes (-1 \ 0 \ 1) = (R_{n-1} \otimes W_{n-1}) \otimes (-1 \ 0 \ 1)$$

which is $R_n \otimes W_n$. Since $R_1 \otimes W_1 = -1 \ 0 \ 1$, Theorem 2 is proven by induction.

Theorem 2 provides the first examples that there are code pairs, X , Y and W , Z , not equivalent under G , which satisfy

$$X * Y = W * Z \quad (24)$$

When $n = 1$, i. e., $m = 2$, the resulting solution is degenerate since $R_1(1)$, (the first row of R_1), is identical to $W_1(2)$, (the second row of W_1) and $R_1(2) = \overleftarrow{W_1(1)}$. It is true that $R_1(1) * W_1(1) = R_1(2) * W_1(2)$ but the same result is obtained by applying Eq. (7) which is one of the invariant statements under G ; $R_1(1) * W_1(1) = \overleftarrow{W_1(1)} * \overleftarrow{R_1(1)}$. When $n = 2$, i. e., $m = 4$, a non-degenerate solution results

$$(1 \ 1 \ 1 \ 1) * (1 \ -1 \ -1 \ 1) = (1 \ -1 \ 1 \ -1) * (-1 \ -1 \ 1 \ 1) = 1 \ 0 \ -1 \ 0 \ -1 \ 0 \ 1$$

which cannot be obtained by applying any of the group operations. The other two possible pairs of codes with the same correlogram can be obtained from these by applying Eq. (7).

Theorem (2) provides a means for constructing 2^{n-1} code pairs X , Y not equivalent under G , all of which have the same correlogram and hence satisfy Eq. (24). There are therefore,

$$\binom{2^{n-1}}{2} = 2^{n-2} (2^{n-1} - 1) \quad (25)$$

unique solutions to Eq. (24) generated by Theorem (2) when $m = 2^n$. The next section demonstrates that these are not the only solutions for large m .

Let A and B be factor code words for which the following is true:

$$\left. \begin{aligned} B &= \overleftarrow{B} \\ A &= \overleftarrow{A} \end{aligned} \right\} \quad (26)$$

and

$$A \neq B, \overleftarrow{B}, \overleftarrow{\overleftarrow{B}}$$

Then by Eq. 4

$$A * B = \overleftarrow{A} B = A B$$

and

$$B * A' = \overleftarrow{B} A' = \overleftarrow{B}' A = B A = A B$$

which proves the fundamental identity

$$A * B = B * A'; \quad (27)$$

if the conditions of Eq. (26) are satisfied. Define two code matrices R and W:

$$R = \begin{pmatrix} A \times A \\ A \times B \\ B \times A \\ B \times B \end{pmatrix} \quad (28)$$

$$W = \begin{pmatrix} B \times B \\ (B \times A)' \\ (A \times B)' \\ A \times A \end{pmatrix} \quad (29)$$

in loose analogy to R_n and T_n given by Eqs. (20) and (22). It is now possible to prove a theorem which generalizes the results of Theorem 2.

Theorem 3

If R and W are code matrices as defined by Eqs. (28) and (29) where the elements A and B satisfy the constraints of Eq. (26), the correlogram of any row of R and the corresponding row of W is given by $(A * B)^2$. Another way of expressing this result is

$$R \circledast W = (A * B)^2$$

Proof:

The following identity is used in the proof of Theorem (3): $(A \times B)' = A' \times B = A \times B'$. Expand $R \circledast W$ by rows using Theorem C to interchange Kronecker products and correlation.

$$R \circledast W = \begin{pmatrix} A \times A \\ A \times B \\ B \times A \\ B \times B \end{pmatrix} \circledast \begin{pmatrix} B \times B \\ (B \times A)' \\ (A \times B)' \\ A \times A \end{pmatrix} = \begin{matrix} A * B \otimes A * B \\ A * B \otimes B * A' \\ B * A' \otimes A * B \\ B * A' \otimes B * A' \end{matrix}$$

Equation (27) shows that all of the right hand terms are identical, and Theorem (3) is proven:

$$R \otimes W = (A * B)^2 \quad (30)$$

The matrices defined by Eqs. (28) and (29) are called Pseudo-Rademacher-Walsh matrices because of their functional similarity to the Rademacher-Walsh matrices defined by Eqs. (20) and (22).

Although Theorem (3) provides a means of constructing solutions to Eq. (24), it does not demonstrate that these solutions will be different from the ones generated by Eqs. (20) and (22). There can only be solutions when m is even, since $B \neq \overline{B}$ for any code when m is odd. The only possible values for A and B (satisfying Eq. (26)) for $m = 2, 4$ and 6 are given in Table 3 below for codes inequivalent under G . Only these primitive codes need be considered, since all derivative codes can be constructed from them.

	$A = \overline{A}$	$B = \overline{B}$
$n = 2$	1 1	1 -1
$n = 4$	1 1 1 1 1 -1 -1 1	1 1 -1 -1 1 -1 1 -1
$n = 6$	1 1 1 1 1 1 1 1 -1 1 -1 1 1 -1 1 1 -1 1 1 -1 -1 -1 -1 1	1 1 1 -1 -1 -1 1 1 -1 1 -1 -1 1 -1 1 -1 1 -1 1 -1 -1 1 1 -1

Table 3

Primitive Pseudo-Rademacher-Walsh Factor Codes

Since $n = 6$ is not a permissible code length for Rademacher-Walsh codes it is obvious that Theorem (3) generates codes not generated by Theorem (2).

The number of codes of type A of length m is half of the total number of palindromic codes given by Eq. (14) since complementation (an operator in G) converts any code in N_p into another equivalent code in N_p . The number of codes of type B of length m is half the total number of anti-palindromic codes as given by Eq. (15). Thus the number of factor codes of type A or of type B is the same, and is given by N_A or N_B .

$$N_A = N_B = 2^{\frac{m-2}{2}} = 2^{s-1} \quad (m = 2s) \quad (31)$$

and the number of matrix pairs $R \otimes W$ is

$$N_m = N_A N_B = 2^{2s-2} \quad (32)$$

Each of these matrices contributes two solutions to Eq. (24) unique up to an equivalence under G .

Theorems (2) and (3) provide general techniques for constructing solutions to Eq. (24), but they do not exhaust the possible solution pairs. The procedure used in Theorem (3) suggests the following generalization. Let $S_n(i)$ be the i -th symmetric function of order n of the following type. Expand i into its binary representation in n positions,

$$i = x_{n-1} 2^{n-1} + x_{n-2} 2^{n-2} + \dots + x_1 2 + x_0 \quad (33)$$

where $x_j = 0, 1$ and $0 \leq i \leq 2^n - 1$.

Form a function $S_n(i)$ by inserting the code A in the j -th position if $x_j = 1$ and a B if $x_j = 0$. The codes A and B satisfy the constraints of Eq. (26). Define matrices $\mathcal{R}_n$ and $\mathcal{W}_n$, using $S_n(i)$, to be the following

$$\mathcal{R}_n = \begin{pmatrix} S_n(0) \\ S_n(1) \\ \vdots \\ S_n(2^n - 2) \\ S_n(2^n - 1) \end{pmatrix} \quad (34)$$

and

$$\mathcal{W}_n = \begin{pmatrix} \alpha_{2^n-1} S_n(2^n-1) \\ \alpha_{2^n-2} S_n(2^n-2) \\ \vdots \\ \alpha_1 S_n(1) \\ \alpha_0 S_n(0) \end{pmatrix} \quad (35)$$

where $\alpha_i = (-1)^{\beta_i}$ and $\beta_i = \sum_{i=0}^{n-1} x_i$

It is then possible to state the following theorem for the codes generated by matrices $\mathcal{R}$ and $\mathcal{W}$.

Theorem 4

If $\mathcal{R}$ and $\mathcal{W}$ are code matrices as defined by Eqs. (34) and (35) where the elements A and B satisfy the constraints of Eq. (26), the correlogram of any row of $\mathcal{R}$ and the corresponding row of $\mathcal{W}$ is given by $(A * B)^n$; i. e.

$$\mathcal{R} \otimes \mathcal{W} = (A * B)^n$$

Proof:

The i -th row of $\mathcal{R}_n$, $S_n(i)$, is generated by the expansion of i to the radix 2 given by Eq. (33). The corresponding row of $\mathcal{W}$ is $S_n(2^n - 1 - i)$ multiplied by a factor of ± 1 . The expansion of $2^n - 1 - i$ in radix 2 is the complement of i , that is a 0 occurs in $2^n - 1 - i$ wherever a 1 appears in i and vice versa. Therefore by the rule given for the construction of $S_n(i)$ an A occurs in every place in $S_n(2^n - 1 - i)$ where a B occurs in $S_n(i)$ and vice versa. Thus, the correlation of two such terms of Kronecker products would (using Theorem C) be the generalized Kronecker product of n correlations each of which has one factor of A and one of B. The order is determined by whether a 0 or 1 occurs at the corresponding location in the expansion of i . Equation (27) shows that if $(A * B)^n$, which is the product of $S_n(0) * S_n(2^n - 1)$, is to equal all other products a complementation must be made for each occurrence of A in a row of $\mathcal{W}$. Since two ' operations leave a Kronecker product unmodified, it is only necessary to introduce a sign change for a row in $\mathcal{W}$ when the number of A's in that row is odd. α_i is constructed to be $+1$ if the number of A's is even and -1 otherwise. Thus by use of Eq. (27) Theorem (3) is proven.

The number of codes of type A and B is unchanged by increasing the number of factors used in forming $\mathcal{R}$ and $\mathcal{W}$. The number of factor code pairs is still N_m ; given by Eq. (32). The number of complete codes is a function of the number of factors used, n . When $n = 2$, each factor code pair contributes a pair of unique products with the same correlogram. When $n = 3$, four pairs

are generated. For general n , the number of solution pairs for a given choice of factors A and B is 2^{n-1} .

It is not a trivial problem to determine which solution pairs are generated more than once by the procedures given in Theorems (2), (3) and (4).

Summary

The principal algebraic properties of the two-sided correlation function have been developed and illustrated in this paper. This theory has immediate application to problems in which the choice of a code is dependent on its correlation properties. Examples are self-synchronizing systems⁷; radar codes⁸ and crypto applications.³

It seems appropriate to close this paper with one of the unsolved problems concerning correlograms which is of central importance to coding applications. Given a proposed correlogram—does there exist any pair of binary codes which generates that correlogram? This problem, except for special cases, is still unsolved.

Appendix A

Theorem A; The Product Rule:

Let X and Y be binary code words of lengths m and n respectively;

$$X = \sum_{j=0}^{m-1} x_j 10^{m-j-1} \quad (1-a)$$

$$Y = \sum_{i=0}^{n-1} y_i 10^{n-i-1} \quad (2-a)$$

then the two sided correlation function $X * Y$ is given by $\overleftarrow{X} Y$, where $\overleftarrow{X}$ is the mirror reversal of X

$$\overleftarrow{X} = \sum_{j=0}^{m-1} x_j 10^j \quad (3-a)$$

and the multiplication is carried out with a radix greater than m or n so that no carries are generated.

Proof:

$X * Y$ was defined in the text to be the sequence of $m+n-1$ symbols $(X * Y)_k$ where by Eq. (1)

$$(X * Y)_k = A - D$$

When $x_j = \pm 1$ and $y_l = \pm 1$, each agreement of a pair of symbols $x_{n-k+l-1}$ and y_l will contribute 1 when they are the same and -1 when they differ. Thus

$$(X * Y)_k = A - D = \sum_{l=0}^R y_l x_{n-k+l-1} \quad (4-a)$$

where l and $n-k+l-1$ are limited to the range 0 to $n-1$ and 0 to $m-1$ respectively for the elements to be defined. R defines the equivalent bound on l :

$$R = \min[n-1, m-1, m+n-2-k, k]$$

Substituting Eq. (4-a) into Eq. (3) gives an expression for $X * Y$ in terms of the elements of X and Y .

$$X * Y = \sum_{k=0}^{m+n-2} \sum_{l=0}^R y_l x_{n-k+l-1} 10^{m+n-k-2} \quad (5-a)$$

The product of $\overleftarrow{X}$ and Y (using a radix greater than m or n so no carries can be generated) may be formed directly from Eqs. (2-a) and (3-a):

$$\overleftarrow{X} Y = \sum_{j=0}^{m-1} \sum_{i=0}^{n-1} x_{m-j-1} y_i 10^{m+n-j-i-2} \quad (6-a)$$

If all of the terms belonging to a like power of 10, say $m+n-k-2$, in Eq. (6-a) are collected, $k = i+j$ or $j = k-i$ and the k -th term $(\overleftarrow{X} Y)_k$ in Eq. (6-a) becomes

$$(\overleftarrow{X} Y)_k = \sum_{i=0}^S y_i x_{m-k+i-1} 10^{m+n-k-2} \quad (7-a)$$

which is only defined for $i \leq S = R$. Collecting all terms $(\overleftarrow{X} Y)_k$ for $0 \leq k \leq m+n-2$, an expression identical to Eq. (5-a) is obtained, i. e.,

$$X * Y = \overleftarrow{X} Y \quad (8-a)$$

Equation (8) was derived without restriction on the lengths, m and n , of the code words X and Y . Equation (8-a) has been published without proof by the author⁴ and has been discussed for the special case $X = Y$ by Bernfeld et al.^{5, 6}

Corollary A-1

$$X * Y = X' * Y'$$

Proof:

$$X * Y = \overleftarrow{X} Y = \overleftarrow{X} Y' = X' * Y'$$

since multiplying a code by -1 is equivalent to complementation.

Corollary A-2

$$X * Y = \overline{Y * X}$$

Proof:

$$Y * X = \overleftarrow{Y} X = \sum_{k'=0}^{m+n-2} \sum_{\ell'=0}^{R'} x_{\ell'} y_{n-k'+\ell'-1} 10^{m+n-k'-2}$$

where

$$R' = \min[n-1, m-1, m+n-k'-2, k']$$

Therefore

$$\overleftarrow{Y * X} = \sum_{k'=0}^{m+n-2} \sum_{\ell'=0}^{R'} x_{\ell'} y_{n-k'+\ell'-1} 10^{k'} \quad (9-a)$$

If like powers of 10 are equated between Eq. (9-a) and (5-a) by setting $k' = m+n-k-2$ then $R \equiv R'$ and the ranges of ℓ and ℓ' are equal and unchanged by the change of variable. The subscript of y in Eq. (9-a) is changed from $m-k+\ell'-1$ to $-n+1+k+\ell'$ which may be equated to ℓ in a second regrouping of variables since both ℓ and $-n+1+k+\ell'$ are dummy variables over the range of 0 to R . This regrouping of terms shows Eq. (9-a) to be identical to Eq. (5-a) which proves the corollary:

$$X * Y = \overleftarrow{X} Y = \overleftarrow{\overleftarrow{Y} X} = \overleftarrow{Y * X} \quad (10-a)$$

Corollary A-3

$$X * 1 = \overleftarrow{X}$$

$$X * -1 = \overleftarrow{X}'$$

These results follow trivially from Theorem A and Corollary A-2.

Corollary A-4

$$X * aY = aX * Y = a(X * Y)$$

Proof:

$$X * aY = \overleftarrow{X} aY = \overleftarrow{aX} Y = aX * Y = a(X * Y)$$

Corollary A-5

$$X * Y = \overleftarrow{Y} * \overline{X}$$

Proof:

$$X * Y = \overleftarrow{X} Y$$

The indicated multiplication is in the field of reals to a radix large enough that no carries are generated, and is therefore commutative.

$$X * Y = \overleftarrow{X} Y = Y \overleftarrow{X} = \overleftarrow{Y} * \overleftarrow{X}$$

Appendix B

Theorem B; The Shift and Add Rule:

Let X, Y and Z be binary code words of lengths m, n and p respectively, then the correlogram

$$Z * (Y 1 0^r + X)$$

where $r \geq m$ can be expressed in terms of the simple correlograms $Z * X$ and $Z * Y$ as follows

$$Z * (Y 1 0^r + X) = (Z * Y) 1 0^r + Z * X$$

Note: Any positions left unoccupied by the r-shift to the left ($r > m$) of Y are assumed to have a nominal value of 0 without implying that a nonbinary code is being used. The 0 merely signifies the absence of a code symbol and hence of a contribution to the correlogram from that position.

Proof:

Define a new code word $W = Y 10^r + X$,

$$W = \sum_{\ell=0}^{r+n-1} w_{\ell} 10^{r+n-\ell-1} \quad (1-b)$$

or equivalently

$$W = \left\{ \sum_{\ell=0}^{n-1} y_{\ell} + \sum_{\ell=n}^{r-m+n-1} 0 + \sum_{\ell=r-m+n}^{r+n-1} x_{\ell-r+m-n} \right\} 10^{r+n-\ell-1} \quad (2-b)$$

Using the form for W given in Eq. (1-b) compute $Z * W$ directly using Theorem A.

$$Z * W = \sum_{h=0}^{p+r+n-2} \sum_{\ell=0}^{R_0} w_{\ell} z_{p-h+\ell-1} 10^{r+n+p-h-2} \quad (3-b)$$

where

$$R_0 = \min[p-1, r+n-1, p+r+n-h-2, h]$$

If $Z * W$ is computed using the expanded form for W given by Eq. (2-b) an alternate expression for $Z * W$ is obtained.

$$\begin{aligned} Z * W &= \sum_{h=0}^{p+r+n-2} \sum_{\ell=0}^{R_0} y_{\ell} z_{p-h+\ell-1} 10^{p+n+r-h-2} \\ &+ \sum_{h=0}^{p+r+n-2} \sum_{\ell=0}^{R_0} x_{\ell-r+m-n} z_{p-h+\ell-1} 10^{p+n+r-h-2} \end{aligned} \quad (4-b)$$

The first sum in Eq. (4-b) is undefined, i. e., contributes nothing to the elements of $Z * W$, for $h > n+p-2$ since the maximum value which ℓ can assume for y_{ℓ} to still be defined is $n-1$, for which value the subscript on z is 0. This limit on h changes R_0 , the upper bound on ℓ to

$$R'_0 = \min[p-1, n-1, p+n-h-2, h]$$

which makes the first term in Eq. (4-b)

$$\left(\sum_{h=0}^{p+n-2} \sum_{\ell=0}^{R'_0} y_{\ell} z_{p-h+\ell-1} 10^{p+n-h-2} \right) 10^r$$

or

$$(Z * Y) 10^r$$

A similar sequence of arguments shows the second term in Eq. (4-b) to be reducible to $Z * X$. All terms in the indicated sum are undefined for $h < r+n-m$ since the minimum value which ℓ can assume for X_{ℓ} to be defined is 0. Introduce a new variable $h' = h-r-n+m$ so that the second term of Eq. (4-b) becomes:

$$\sum_{h'=0}^{p+m-2} \left(\sum_{\ell=0}^{R''_0} x_{(\ell-r-n+m)} z_{p-h'-1+(\ell-r-n+m)} \right) 10^{m+p-h'-2} \quad (5-b)$$

The term $(\ell-r-n+m)$ is limited to a range of 0 to $m-1$ for $x_{\ell-r-n+m}$ to be defined. Let this variable be a new dummy variable $\ell' = \ell-r-n+m$ then

$$R''_0 = \min[p-1, m-1, p+m-h'-2, h']$$

and the second term of Eq. (5-b) is identical in form to Eq. (5-a) for $X * Y$.

Therefore:

$$Z * (Y 10^r + X) = (Z * Y) 10^r + Z * X$$

with no restrictions on the lengths m , n , and p of the codes X , Y , and Z for any left shift $r \geq m$.

It should be noted that while the restriction that $r \geq m$ is adequate to guarantee that no elements of X and the shifted code word $Y 10^r$ overlap and hence must be added, that the same is not true for the correlograms $Z * X$ and $(Z * Y) 10^r$. These correlograms will have an overlap of $p+m-r$ symbols unless $r > p+m$. In particular, the case which is of greatest interest, $r = m$, results in an overlap between the correlograms of p symbols.

Corollary B-1

$$Z * (Y 10 + 1) = (Z * Y) 10 + \overline{Z}$$

$$Z * (Y 10 - 1) = (Z * Y) 10 + \underline{Z}$$

This result follows trivially from Theorem B and Corollary A-3. It is included because it provides an alternate algorithm for computing correlograms, which is especially useful if one has a table for codes of length m and wishes to generate some cases of length $m+1$. The correlogram for any code pair $Z * (Y 10 \pm 1)$ can be constructed by shifting the correlogram obtained for $Z * Y$ to the left one position and adding either the reversed code or its complement, depending on whether the right-hand-most symbol of the new code is ± 1 .

Corollary B-2

Let X be a code word, m symbols in length. Its correlogram with the code word Z can be represented as follows, with any partitioning $m = p_1 + p_2 + \dots + p_n$

$$\begin{aligned} Z * X &= \left(\left(x_0 \dots x_{p_1-1} \right) \left(x_{p_1} \dots x_{p_1+p_2-1} \right) \dots \left(x_{\sum p_j} \dots x_{m-1} \right) \right) \\ &= Z * \left(x_0 \dots x_{p_1-1} \right) 10^{m-p_1} + Z * \left(x_{p_1} \dots x_{m-1} \right) \\ &= Z * \left(X_1 \right) 10^{m-p_1} + Z * \left(x_{p_1} \dots x_{m-1} \right) \end{aligned}$$

which can be repeated n times to obtain

$$Z * X = \sum_{i=1}^n (Z * X_i) 10^{m-i}$$

where X_i represents the factored elements in the i -th partition.

Corollary B-3

$$(Y 10^r + X) * Z = (Y * Z) 10^r + X * Z$$

where $r \geq m$.

Proof:

This result follows by first applying Theorem A and then Theorem B to the left-hand expression,

$$\begin{aligned} (Y 10^r + X) * Z &= \overline{Z * (Y 10^r + X)} \\ &= \overline{(Z * Y) 10^r + Z * X} \\ &= \overline{(Z * Y) 10^r} + \overline{Z * X} \\ &= (Y * Z) 10^r + X * Z \end{aligned}$$

Appendix C

Theorem C; The Kronecker Product Rule:

Let X and Y be binary code words, of lengths m and n respectively. X is the Kronecker product^Δ of two factors U and V of lengths k and ℓ and Y is the product of W and Z of lengths p and r :

$$X = U \times V \text{ where } K\ell = m \quad \text{and} \quad Y = W \times Z \text{ where } pr = n$$

^ΔDefinition: The Kronecker product, $U \times V$, of the codes

$$U = \sum_{j=0}^{k-1} u_j 10^{k-j-1} \quad \text{and} \quad V = \sum_{i=0}^{\ell-1} v_i 10^{\ell-i-1}$$

is given by the summation

$$U \times V = \sum_{j=0}^{k-1} u_j V 10^{k\ell - (j+1)\ell}$$

The base 10 is used only as a positional rotation for the code symbols. $U \times V$ has $m = k\ell$ symbols.

The correlogram $X * Y$ can be expressed in terms of the correlograms $V * Z$ and $U * W$ as follows:

$$X * Y = \sum_{i=0}^{k+p-2} (U * W)_i (V * Z) 10^{m+n-ir-2r}$$

when $\ell = r$. The summation is made with a radix greater than m or n so that no carries can be generated.

Proof:

Since X is the Kronecker product of U and V , it may be written

$$X = \sum_{j=0}^{k-1} u_j V 10^{m-j\ell-\ell} \quad (1-c)$$

similarly, Y may be represented as

$$Y = \sum_{j'=0}^{p-1} w_{j'} Z 10^{n-j'r-r} \quad (2-c)$$

Equation (2-c) may be used to expand $X * Y$ into the form

$$X * Y = X * \left(\sum_{j'=0}^{p-1} w_{j'} Z 10^{n-j'r-r} \right)$$

which may be rewritten with the powers of ten brought outside the operator (by Corollary B-2) since a code word of length r is being left shifted r positions each time. Therefore

$$X * Y = \sum_{j'=0}^{p-1} (X * w_{j'} Z) 10^{n-j'r-r} \quad (3-c)$$

but by Corollary A-4 Eq. (3-c) can be written in the form

$$X * Y = \sum_{j'=0}^{p-1} w_{j'} (X * Z) 10^{n-j'r-r} \quad (4-c)$$

Equation (1-c) may be substituted into Eq. (4-c) and Corollary B-2 used again to obtain the equation:

$$X * Y = \sum_{j=0}^{k-1} \sum_{j'=0}^{p-1} u_{k-1-j} w_{j'} (V * Z) 10^{m+n-j\ell-j'r-\ell-r} \quad (5-c)$$

where the conditions on X for Theorem B to be applicable are satisfied since a code word of length ℓ is being left shifted ℓ positions each time. Equation (5-c) is valid in general.

The expression for $(U * W)_i$ is

$$(U * W)_i = \sum_{\alpha=0}^R w_{\alpha} u_{k-i-1+\alpha} \quad (6-c)$$

where

$$U * W = \sum_{i=0}^{k+p-2} (U * W)_i 10^{k+p-2-i}$$

and

$$R = \min[k-1, p-1, k+p-2-\alpha, \alpha]$$

A necessary and sufficient condition for the indicated summation of terms $u_{k-1-j} w_{j'}$ in Eq. (5-c) to give rise to $(U * W)_i$ is that $r = \ell$. Sufficiency is easy to demonstrate, for if $r = \ell$, then the shifting operator in Eq. (5-c) becomes:

$$10^{m+n-j\ell-j'r-\ell-r} = 10^{(m+n-\ell-r) - r(j+j')}$$

which reduces to

$$10^{m+n-ir-2r}$$

upon equating subscripts in Eqs. (5-c) and (6-c), which implies

$$i = j+j'$$

Therefore if $r = \ell$

$$X * Y = \sum_{i=0}^{k+p-2} (U * W)_i (V * Z) 10^{m+n-ir-2r} \quad (7-c)$$

Necessity is slightly more difficult to demonstrate. The number of symbols in $X * Y$ when computed directly by Theorem A and indirectly by Theorem C must be the same, i. e.,

$$k\ell + pr - 1 = q(k+p-2) + \ell + r - 1$$

where q is an as yet unspecified shift factor.

In Equation (5-c) let $i = j + j'$ to obtain as the general expression for the i -th term of $X * Y$

$$(X * Y)_i = \sum_{j=0}^{k-1} u_{k-j-1-i} w_i 10^{(\ell-r)(k-j-1)}$$

which is identical to Equation (6-c) for arbitrary u_j and w_i only if $r = \ell$ so that the exponent is identically 0, i. e., if $q = r = \ell$. Therefore Equation (7-c) is valid if and only if $r = \ell$ as was to be shown.

Corollary C-1^Δ

One especially interesting case in which the conditions for Theorem C to apply are satisfied is when $X = Y$ so that $X * Y = X * X$ is the autocorrelogram (not the cyclic autocorrelation function) of a code word which is representable as

^ΔThe results given in Corollaries C-1 and C-2 have been published⁴ by the author without proof.

a Kronecker product. If $X = U \times V$, X , U , and V are of lengths m , k , and ℓ respectively, then

$$X * X = (U * U) \otimes (V * V)$$

where $\otimes$ is a generalization ^{Δ} of the Kronecker product defined below.

Proof:

This result follows by replacing W and Z by U and V in Equation (7-c) and noting that the shift and add operator is precisely that described for $\otimes$.

Corollary C-2

If $X = U_1 \times U_2 \times \dots \times U_n$ then the autocorrelogram $X * X$ is given by

$$X * X = (U_1 * U_1) \otimes (U_2 * U_2) \otimes \dots \otimes (U_n * U_n)$$

where no restrictions on the lengths of the factors U_i need be made.

Proof:

Apply Corollary C-1 n times, operating on the right-hand-most factor each time.

^{Δ} Definition: The Kronecker product $U \times V$ of a pair of code words U and V of lengths k and ℓ respectively as defined earlier by the summation formula may be interpreted to consist of k shifts to the left of ℓ positions at a time of V , complemented or uncomplemented depended on the value of the corresponding symbol in U , and its addition to form a new code word of length $m = k\ell$ as represented by Equation (1-c). The generalized Kronecker product $\otimes$ preserves this multiply, shift and add property, independent of the length of the symbol sequences being operated upon, and is defined by

$$(U * U) \otimes (V * V) = \sum_{i=0}^{2k-2} (U * U)_i (V * V) 10^{(2k-i-2)\ell}$$

In this form $\otimes$ is the same sequence of operations on correlograms as X is on the corresponding factor codes, which says that the generalized Kronecker product commutes with the $*$ operator.

References

1. L. Baumert, M. Easterling, S. W. Golomb, and A. Viterbi, "Coding Theory and Its Applications to Communications Systems," Technical Report 32-67, Jet Propulsion Laboratories, Pasadena, Calif., March 31, 1961.
2. S. W. Golomb, Digital Communications with Space Applications, Prentice-Hall, Englewood Cliffs, N. J., 1964.
3. S. W. Golomb, Shift Register Sequences, Holden-Day, Inc., San Francisco Calif., 1967.
4. G. J. Simmons, "A Factorization Technique for Binary Autocorrelation Functions," Proceedings of the IEEE, Vol. 54, No. 5, May 1966, pp. 794-795.
5. M. Bernfeld, "A Property of Binary Sequences," Proceedings of the IEEE, Vol. 52, June 1964, p. 744.
6. P. M. Liebman and M. Bernfeld, "On a Property of Binary Sequences," Proceedings of the IEEE, Vol. 53, April 1965, p. 409.
7. R. H. Barker, "Group Synchronizing of Binary Digital Systems," Communication Theory edited by W. Jackson, Butterworths, London, 1953.
8. R. Turyn and J. Storer, "On Binary Sequences," Proceedings of the American Mathematical Society, Vol. 12, 1961, pp. 394-399.

This work was supported by the U. S. Atomic Energy Commission.