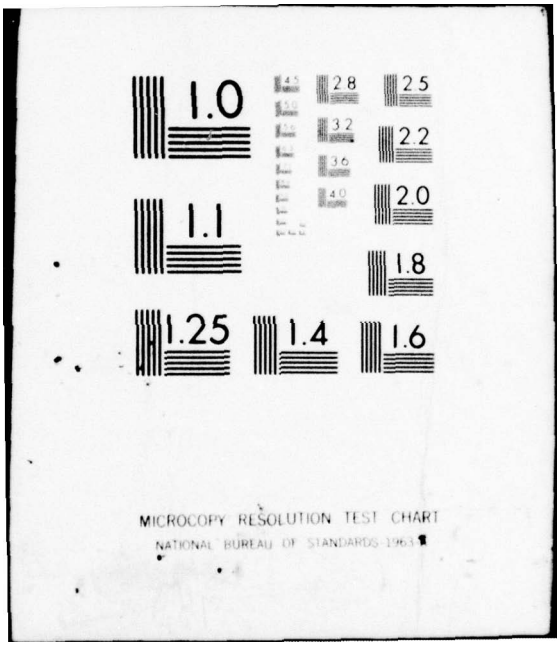
AD-A034 033 NAVAL RESEARCH LAB WASHINGTON D C F/G 9/4
MEAN AND VARIANCE OF THE CORRELATION MAGNITUDE OF RANDOM AND PS--ETC(U)
NOV 76 L S BEARCE, A J ZIFFER

UNCLASSIFIED NRL-8068 NL

1 OF 1
AD
A034033

END

DATE
FILMED
2-77


1.0
2.8
2.5
3.2
2.2
3.6
2.0
4.0
1.1
1.8
1.25
1.4
1.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963

NRL Report 8068

Mean and Variance of the Correlation Magnitude of Random and Pseudonoise Sequences

LOREN S. BEARCE AND ARTHUR J. ZIFFER

Satellite Communication Branch
Communications Sciences Division

November 24, 1976

NAVAL RESEARCH LABORATORY
Washington, D.C.

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: NRL [illegible] 8068	2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER	
4. TITLE (and Subtitle): MEAN AND VARIANCE OF THE CORRELATION MAGNITUDE OF RANDOM AND PSEUDONOISE SEQUENCES	5. TYPE OF REPORT & PERIOD COVERED: An interim report on a continuing NRL problem
6. PERFORMING ORG. REPORT NUMBER	
7. AUTHOR(s): Loren S. Bearce, Arthur J. Ziffer	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS: Naval Research Laboratory, Washington, DC 20375	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: NRL Problem R01-82, Project JSB-06, 1121
11. CONTROLLING OFFICE NAME AND ADDRESS: Department of the Navy, Strategic Systems Project Office, Washington, DC 20376	12. REPORT DATE: Nov[illegible]976
	13. NUMBER OF PAGES: 28
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)	15. SECURITY CLASS. (of this report): Unclassified
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Binary sequences	Crosscorrelation
Code characteristics	Psuedonoise codes
Communications, spread-spectrum	Sequences

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The mean or expected value and the variance of the *absolute value* of correlation between equal-length independent random sequences have been determined and compared with the same measures for full-period pseudonoise (PN) sequences, which have applied extensively in spread-spectrum radio communications systems. The magnitude of correlation is often of primary interest in such applications, since a strong negative correlation is as significant as a strong positive correlation; hence correlation detectors exist which function on the basis of the magnitude of correlation. The comparison reveals several advantages of the Gold codes which are due to their inherent

(Continued) over

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

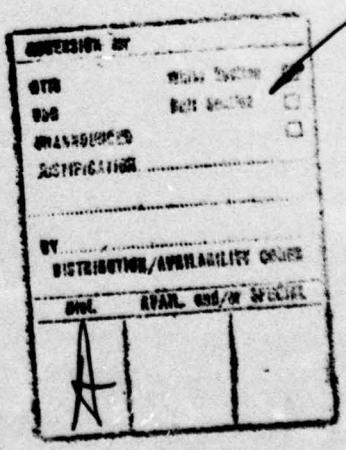
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

251950

20

mutual orthogonality. The study of random codes permits the performance evaluation of such detectors during periods of noise-only input and also provides a long-needed point of reference for PN system design.

CONTENTS



MEAN AND VARIANCE OF THE CORRELATION MAGNITUDE OF RANDOM AND PSEUDONOISE SEQUENCES

INTRODUCTION

The mean or expected value and the variance of the *absolute value* or *magnitude* of the correlation between two equal-length independent random sequences are derived for all unique bit-integral relative phase conditions. These are then compared with the same measures for the full-period correlation between pairs of certain specific types of pseudonoise (PN) sequences which have been applied extensively in spread-spectrum radio-communications systems. The study of independent random sequences reported here provides a long-needed point-of-reference for designers of spread-spectrum systems, because the autocorrelation and crosscorrelation properties of candidate PN sequences may now be compared with the same quantities derived for fundamental random sequences. Correlation detectors exist which function on the basis of the magnitude of correlation between a receiver input and an internally generated reference sequence. The treatment of random sequences presented here permits evaluation of the performance characteristics of such detectors during periods of noise-only input.

Design studies, validated by measurements of hardware implementation, have proved that differentially coherent phase-shift-keyed (DPSK) modulation formats permit realization of a relatively high communications efficiency for digital radio-communications systems when interference is an insignificant problem. An important motivation for the development of spread-spectrum techniques stems from the need to mitigate the effects of severe electromagnetic interference. Spread-spectrum systems have been developed which reduce interference significantly and approach the same communications efficiencies demonstrated by DPSK systems.

Spread-spectrum systems employ an encoding digital bit stream upon which baseband informational data are impressed as a modulation. The baseband information can be recovered in the demodulation process only by correlation with a properly synchronized replica of the encoding signal; however the correlation process permits a discrimination against the uncorrelated intervening interference. Certain reproducible, deterministic, pseudorandom sequences which provide the wideband low-power-density encoding signals needed for such systems tend to optimize the use of the communications capacity offered by a channel with noise and interference. These sequences have statistical properties similar to noise and hence are known as pseudonoise (PN) sequences.

The usefulness of PN sequences as codes in spread-spectrum communications depends on both their individual autocorrelation and their joint crosscorrelation properties. Autocorrelation properties are important for assuring rapid and proper synchronization of the incoming signal with the locally generated replica of the PN encoding sequence. To

---

Manuscript submitted August 16, 1976.

perform the synchronization, a scanning or time search between the incoming signal and the local PN sequence (often generated by a binary shift-register code generator) is required. Sequences with off-peak autocorrelation values comparable to the main correlation peak are undesirable, because they tend to confuse the synchronization process and prevent the full interference discrimination or processing gain realizable with proper synchronization. The crosscorrelation properties of the sequences are of considerable significance in multiplexing applications in which many communications systems must operate in a common frequency channel, with each communication link employing a different PN sequence. The crosscorrelation between any two sequences used in the system must be sufficiently low to provide the particular amount of interference isolation required between the multiplexed channels for satisfactory operation.

Prior studies by others have considered the statistical nature of only the correlation function itself for various sequences. However the properties of the *absolute value* of the correlation function are often of primary interest in applications such as spread-spectrum communications, where a strong negative correlation is equally as significant as a strong positive correlation. Gold [1, 2] has developed a method of selecting certain special maximal-length linear PN sequences which he used in pairs and called *preferred pairs*. A maximal-length sequence is the longest which can be repetitively generated by a given size code generator. The least upper bound of the absolute values (or magnitudes) for the crosscorrelation of these maximal-length preferred pairs is better (smaller) than for any other two arbitrarily chosen maximals of the same length (except for some minor exceptions which have peaks only slightly less than that bound). Because these special codes were originally identified by Gold and are most often used in sets of two, they are commonly referred to as Gold pairs. Further, and of considerable significance for practical applications, Gold [1, 2] proved that these same low crosscorrelation magnitude bounds exist for large families or related encoding sequences, known as Gold code families, where each member of a family may be generated by forming modulo-2 linear combinations of a Gold pair of sequences. Such codes have the same period as the Gold pair used to generate them. The bound for the magnitude of crosscorrelation between any two members of a Gold family of sequences thus can be characterized by just the bound appropriate for the Gold pair used to generate the family.

Since a statistical analysis of the properties of the magnitude of correlation for all possible phase shifts of two purely random sequences apparently has not been developed and presented previously, expressions are derived for the expected value and variance of the full-period correlation magnitude values for each relative phase relationship between a synchronized random sequence and another independent code of the same length. (If a binary sequence is random and independent of another, the expected correlation magnitude between the two is independent of the specific nature of the other, because in either case the probability of matching any pair of bits is 1/2. Furthermore the expected crosscorrelation magnitudes for two independent random sequences is therefore the same as their individual expected autocorrelation magnitudes, for the same reasons.) Random code lengths corresponding to maximal-length PN sequences have been selected for study to facilitate a direct comparison of their respective characteristics. The analysis provided by this study is applicable to bit-synchronized data with negligibly small Doppler-frequency effects. The crossspectral correlation characteristics which are discussed in Figs. 3 and 4 for nonsynchronized data with significant relative Doppler-frequency shifts are not treated here.

DERIVATION OF THE EXPECTED VALUE FOR THE MAGNITUDE OF THE CORRELATION BETWEEN TWO RANDOM SEQUENCES

For time-dependent periodic functions $f(t)$ and $g(t)$ of period T, the normalized crosscorrelation $R(\tau)$ between them is

$$R(\tau) = \frac{1}{T}\int_0^T f(t)g(t+\tau)\,dt. \tag{1}$$

The functions $f(t)$ and $g(t)$ of the continuous variable t are now replaced with the functions $a(i)$ and $b(i)$ of a discrete variable i (which is a common form for describing sequences), so that the crosscorrelation may be expressed in the analogous discrete form

$$R(j) = \frac{1}{L}\sum_{i=1}^{L} a(i)b(i+j), \tag{2}$$

where the $a(i)$ and $b(i+j)$ values are taken from the set $\{+1, -1\}$ and L is the number of discrete elements in the period. Hence

$$\begin{aligned} a(i)b(i+j) &= +1, \text{ if } a(i) = b(i+j), \\ &= -1, \text{ if } a(i) \neq b(i+j). \end{aligned} \tag{3}$$

If n represents the number of agreements, then $L - n$ will represent the number of disagreements; and $R(j)$ can be written as

$$R(j) = \frac{1}{L}\left[\sum_{\substack{i \\ a(i)=b(i+j)}} a(i)b(i+j) + \sum_{\substack{i \\ a(i)\neq b(i+j)}} a(i)b(i+j)\right] \tag{4}$$

$$= \frac{1}{L}\left[\sum_{\substack{i \\ a(i)=b(i+j)}} a(i)b(i+j) - \sum_{\substack{i \\ a(i)\neq b(i+j)}} |a(i)b(i+j)|\right] \tag{5}$$

$$= \frac{1}{L}\left[n - (L-n)\right]. \tag{6}$$

The expression in brackets in (6) is the form given by Gold [1, 2] for the correlation, namely, the number of agreements minus the number of disagreements. The multiplicative factor $(1/L)$ normalizes the correlation. Following Gold [1, 2] θ will be used to represent the normalized discrete correlation $\theta(n)$, (where the discrete variable n here represents the number of agreements between the two sequences, rather than a particular phase shift of the second sequence). Thus

$$\theta(n) = (2n/L) - 1. \tag{7}$$

Given two sequences of the same length, if at least one sequence is random and independent of the other, the probability of an agreement between any two corresponding bits is 1/2. Hence the probability of n agreements arranged in a particular order is $(1/2)^n$. Similarly the probability of $L - n$ disagreements occurring in a particular order is $(1/2)^{L-n}$. With use of the binomial coefficient, namely,

$$\binom{L}{n} = \frac{L!}{n!\,(L-n)!} = \frac{L!}{(L-n)!\,n!} = \binom{L}{L-n}, \tag{8}$$

which is the number of different ways of obtaining n agreements and $L - n$ disagreements, the probability of getting exactly n agreements in any order is

$$p(n) = \binom{L}{n}\left(\frac{1}{2}\right)^n\left(\frac{1}{2}\right)^{L-n}$$

$$= \binom{L}{n}\left(\frac{1}{2}\right)^L. \tag{9}$$

The expected value $E(|\theta|)$, or mean μ, of the absolute value of the correlation is the sum of each of the possible values of $|\theta(n)|$, weighted by the corresponding probability of occurrence for each case. Thus

$$\mu = E|\theta| = \sum_{n=0}^{L} |\theta(n)|p(n).$$

$$= \sum_{n=0}^{L} \left|\frac{2n}{L} - 1\right| \left[\binom{L}{n}\left(\frac{1}{2}\right)^L\right]$$

$$= \left(\frac{1}{2}\right)^L \sum_{n=0}^{L} \left|\frac{2n}{L} - 1\right| \binom{L}{n}. \tag{10}$$

By definition of the absolute value,

$$\left|\frac{2n}{L} - 1\right| = 1 - \frac{2n}{L}, \quad \text{if } 0 \leq n \leq K,$$

$$= \frac{2n}{L} - 1, \text{ if } K + 1 \leq n \leq L, \tag{11}$$

where

$$K = \frac{L-1}{2}, \quad L \text{ odd},$$

$$= \frac{L-2}{2}, \quad L \text{ even}. \tag{12}$$

Thus (10) can be written

$$\mu = \left(\frac{1}{2}\right)^L \left[\sum_{n=0}^{K} \left(1 - \frac{2n}{L}\right)\binom{L}{n} + \sum_{n=K+1}^{L} \left(\frac{2n}{L} - 1\right)\binom{L}{n} \right]. \tag{13}$$

Let $m = L - n$; then, by use of (8), the second summation in (13) becomes

$$\sum_{n=K+1}^{L} \left(\frac{2n}{L} - 1\right)\binom{L}{n} = \sum_{m=L-(K+1)}^{0} \left[\frac{2(L-m)}{L} - 1\right]\binom{L}{m}$$

$$= \sum_{m=}^{0} \left(1 - \frac{2m}{L}\right)\binom{L}{m}, \quad L \text{ odd},$$

$$= \sum_{m=K+1}^{0} \left(1 - \frac{2m}{L}\right)\binom{L}{m}, \quad L \text{ even},$$

which, after the index m is replaced with n, becomes

$$\sum_{n=K+1}^{L} \left(\frac{2n}{L} - 1\right)\binom{L}{n} = \sum_{n=0}^{K} \left(1 - \frac{2n}{L}\right)\binom{L}{n}, \quad L \text{ odd},$$

$$= \sum_{n=0}^{K+1} \left(1 - \frac{2n}{L}\right)\binom{L}{n} = \sum_{n=0}^{K} \left(1 - \frac{2n}{L}\right)\binom{L}{n}, \quad L \text{ even},$$

$$= \sum_{n=0}^{K} \left(1 - \frac{2n}{L}\right)\binom{L}{n}, \quad L \text{ odd or even}. \tag{14}$$

The summand for $n = K + 1$ is neglected for L even because this summand is 0; that is, if

$$n = K + 1 = \left(\frac{L-2}{2}\right) + 1 = \frac{L}{2},$$

then

$$\left(1 - \frac{2n}{L}\right) = 1 - \frac{2}{L}\left(\frac{L}{2}\right) = 0. \tag{15}$$

Substitution of (14) in (13) gives

$$\mu = \left(\frac{1}{2}\right)^L \left[2\sum_{n=0}^{K}\left(1-\frac{2n}{L}\right)\binom{L}{n}\right]$$

$$= \left(\frac{1}{2}\right)^{L-1}\left[\sum_{n=0}^{K}\binom{L}{n} - \sum_{n=1}^{K}\frac{2n}{L}\binom{L}{n}\right], \tag{16}$$

where in the second summation the lower index becomes 1 instead of 0 because n is a multiplicative factor.

The binomial expansion

$$(a+b)^p = \sum_{i=0}^{p}\binom{p}{i}a^{p-i}b^i \tag{17}$$

becomes, for $a = b = 1/2$,

$$1 = \sum_{i=0}^{p}\binom{p}{i}\left(\frac{1}{2}\right)^p$$

$$= \left(\frac{1}{2}\right)^p\sum_{i=0}^{p}\binom{p}{i}, \tag{18}$$

which can be written

$$2^p = \sum_{i=0}^{p}\binom{p}{i}. \tag{19}$$

In the notation desired here, (19) is written as

$$2^L = \sum_{n=0}^{L}\binom{L}{n}$$

$$= \sum_{n=0}^{K}\binom{L}{n} + \sum_{n=K+1}^{L}\binom{L}{n}, \tag{20}$$

which, by use of (12) and $m = L - n$, can be written as

$$2^L = \sum_{n=0}^{K}\binom{L}{n} + \sum_{m=K}^{0}\binom{L}{m}, \quad L \text{ odd},$$
$$= \sum_{n=0}^{K}\binom{L}{n} + \sum_{m=K+1}^{0}\binom{L}{m}, \quad L \text{ even}. \tag{21}$$

Then, if the arbitrary index m is replaced by n and the order of summation, is reversed, (21) becomes

$$2^L = \sum_{n=0}^{K}\binom{L}{n} + \sum_{n=0}^{K}\binom{L}{n}, \quad L \text{ odd},$$
$$= \sum_{n=0}^{K}\binom{L}{n} + \sum_{n=0}^{K+1}\binom{L}{n}, \quad L \text{ even}, \tag{22}$$

or

$$2^L = 2\sum_{n=0}^{K=(L-1)/2}\binom{L}{n}, L \text{ odd},$$
$$= 2\sum_{n=0}^{K=(L-2)/2}\binom{L}{n} + \binom{L}{L/2}, L \text{ even}. \tag{23}$$

Also, from the definition of the binomial coefficient,

$$\frac{n}{L}\binom{L}{n} = \binom{n}{L}\left[\frac{L!}{n!(L-n)!}\right]$$
$$= \frac{(L-1)!}{(n-1)![(L-1)-(n-1)]!}$$
$$= \binom{L-1}{n-1}. \tag{24}$$

Use of (23) and (24) in (16) yields

$$\mu = \left(\frac{1}{2}\right)^{L-1}\left[2^{L-1} - 2\sum_{n=1}^{K}\binom{L-1}{n-1}\right], \; L \text{ odd},$$

$$= \left(\frac{1}{2}\right)^{L-1}\left[2^{L-1} - \frac{1}{2}\binom{L}{L/2} - 2\sum_{n=1}^{K}\binom{L-1}{n-1}\right], \; L \text{ even}. \tag{25}$$

If

$$M = n - 1 \tag{26}$$

is introduced, then

$$\sum_{n=1}^{K}\binom{L-1}{n-1} = \sum_{m=0}^{K-1}\binom{L-1}{M}, \tag{27}$$

where

$$K - 1 = \frac{L-3}{2}, \; L \text{ odd},$$

$$= \frac{L-4}{2}, \; L \text{ even}. \tag{28}$$

When L is even, $L - 1$ is odd, and vice versa; therefore if (23), is applied, to the case in which L is replaced by $L - 1$, it can be written as

$$2^{L-1} = 2\sum_{n=0}^{(L-3)/2}\binom{L-1}{n} + \binom{L-1}{\frac{L-1}{2}}, \quad L \text{ odd},$$

$$= 2\sum_{n=0}^{(L-2)/2}\binom{L-1}{n}, \quad L \text{ even}. \tag{29}$$

Thus

$$2\sum_{M=0}^{K-1}\binom{L-1}{M} = 2^{L-1} - \binom{L-1}{\frac{L-1}{2}}, \quad L \text{ odd},$$

and

$$2\sum_{M=0}^{K-1}\binom{L-1}{M} = 2\left[\sum_{M=0}^{K=(L-2)/2}\binom{L-1}{M} - \binom{L-1}{\frac{L-2}{2}}\right] = 2^{L-1} - 2\binom{L-1}{\frac{L-2}{2}}, \; L \text{ even.} \tag{30}$$

Substituting (30) into (25) and using (27),

$$\mu = \left(\frac{1}{2}\right)^{L-1}\left[2^{L-1} - 2^{L-1} + \binom{L-1}{\frac{L-1}{2}}\right], \; L \text{ odd,}$$

$$= \left(\frac{1}{2}\right)^{L-1}\left[2^{L-1} - \frac{1}{2}\binom{L}{\frac{L}{2}} - 2^{L-1} + 2\binom{L-1}{\frac{L-2}{2}}\right], \; L \text{ even.} \tag{31}$$

For L even, the expression in brackets may be simplified using (8):

$$\mu = \left(\frac{1}{2}\right)^{L-1}\left[2\binom{L-1}{\frac{L-2}{2}} - \frac{1}{2}\binom{L}{\frac{L}{2}}\right] = \left(\frac{1}{2}\right)^{L}\left[\frac{4\left(\frac{L}{2}\right)(L-1)!}{\left(\frac{L}{2}\right)\left(\frac{L}{2}-1\right)!\left(\frac{L}{2}\right)!} - \frac{L!}{\left[\left(\frac{L}{2}\right)!\right]^2}\right]$$

$$= \left(\frac{1}{2}\right)^{L}\frac{L!}{\left[\left(\frac{L}{2}\right)!\right]^2}, \; L \text{ even.} \tag{32}$$

Thus

$$\mu = E(|\theta|) = \left(\frac{1}{2}\right)^{L-1}\binom{L-1}{\frac{L-1}{2}}, \; L \text{ odd,}$$

$$= \left(\frac{1}{2}\right)^{L}\binom{L}{\frac{L}{2}}, \; L \text{ even.} \tag{33}$$

In expanded form $\mu = 1$ for $L = 1$ and for $L \geq 2$,

$$\mu = \left(\frac{1}{2}\right)\left(\frac{3}{4}\right)\left(\frac{5}{6}\right)\cdots\left(\frac{L-2}{L-1}\right), L \text{ odd},$$

$$= \left(\frac{1}{2}\right)\left(\frac{3}{4}\right)\left(\frac{5}{6}\right)\cdots\left(\frac{L-1}{L}\right), L \text{ even}. \tag{34}$$

By use of Stirling's approximation for factorials namely,

$$m! \approx e^{-m} m^m (2\pi m)^{1/2}, \tag{35}$$

the following approximate evaluations for (33), valid for $L >> 1$, can be obtained;

$$\mu \approx \frac{(1/2)^m \left[e^{-m} m^m (2\pi m)^{1/2}\right]}{\left[e^{-m/2}\left(\frac{m}{2}\right)^{m/2}\left(2\pi\frac{m}{2}\right)^{1/2}\right]^2} \approx \left(\frac{2}{\pi m}\right)^{1/2},$$

where

$$2 \leq m = L-1, L \text{ odd},$$

$$= L, L \text{ even}. \tag{36}$$

This approximate relationship is particularly useful when L is very large, because the direct evaluation of (34) takes excessive computer time. Table 1 presents a test program for comparing (33), or (34), with (36) for several sequences of period $L = 2^N - 1$, where N is a positive integer corresponding to the number of stages in a binary shift-register code generator. The results, shown in Table 2, indicate that (36) becomes a progressively better approximation as N (and L) increases and that the error is negligible (less than 0.0003 dB) for $L = 10{,}000$ or more.

DERIVATION OF THE VARIANCE OF THE MAGNITUDE OF THE CORRELATION BETWEEN TWO RANDOM SEQUENCES

The variance σ^2 of the absolute value of the correlation about the mean value is defined as the sum of the squares of the deviations from the mean, weighted by the probability of occurrence for each case. Thus, by use of (7) and (10) and, by definition,

$$\sum_{n=0}^{L} p(n) = 1,$$

Table 1 — FORTRAN Program to Validate the Approximation Given by (36)

```
00100 PROGRAM STIRL(OUTPUT)
00110 PRINT,*        N        L       TRUE    APPROX.          ERROR*,
00120+/,     *                          VALUE     VALUE          IN DB*,/
00130 DO 10 N=3,17
00140 L=2**N-1
00150 CALL AVT(L,E)
00160 CALL XAVT(L,T)
00170 DDB=20.*ALOG10(T/E)
00180 PRINT 20,N,L,E,T,DDB
00190 10 CONTINUE
00200 20 FORMAT(2I8,2F10.6,E12.5)
00210 END
00220C
00230C
00240 SUBROUTINE AVT(L,E)
00250 J=L
00260 E=L/2
00270 K=E*2.
00280 IF(K.EQ.L) J=J+1
00290 K=0
00300 J=(J-1)/2
00310 E=1.
00320 DO 10 I=1,J
00330 X=K=K+1   $   Y=K=K+1
00340 E=E*X/Y
00350 10 CONTINUE
00360 RETURN
00370 END
00380C
00390C
00400 SUBROUTINE XAVT(L,T)
00410 B=0.636619772365755
00420 J=L
00430 A=L/2
00440 K=A*2.
00450 IF(K.EQ.L) J=J+1
00460 A=J-1
00470 T=SQRT(B/A)
00480 RETURN
00490 END
```

Table 2 — Computed Results of the Validation Program *of* Table 1

N	L	TRUE VALUE	APPROX. VALUE	ERROR IN DB
3	7	.312500	.325735	.36029E+00
4	15	.209473	.213244	.15497E+00
5	31	.144464	.145673	.72369E-01
6	63	.100924	.101331	.35022E-01
7	127	.070940	.071081	.17234E-01
8	255	.050014	.050064	.85491E-02
9	511	.035314	.035331	.42578E-02
10	1023	.024952	.024958	.21247E-02
11	2047	.017637	.017640	.10613E-02
12	4095	.012469	.012470	.53040E-03
13	8191	.008816	.008817	.26514E-03
14	16383	.006234	.006234	.13255E-03
15	32767	.004408	.004408	.66273E-04
16	65535	.003117	.003117	.33136E-04
17	131071	.002204	.002204	.16570E-04

the variance is

$$\sigma^2 = \sum_{n=0}^{L} (|\theta(n)| - \mu)^2 p(n) \tag{37}$$

$$= \sum_{n=0}^{L} [\theta(n)]^2 p(n) - 2\mu \sum_{n=0}^{L} |\theta(n)|\, p(n) + \mu^2 \sum_{n=0}^{L} p(n)$$

$$= \sum_{n=0}^{L} \theta^2(n) p(n) - 2\mu(\mu) + \mu^2(1)$$

$$= \sum_{n=0}^{L} \theta^2(n) p(n) - \mu^2 \tag{38}$$

$$\sigma^2 = \sum_{n=0}^{L} \left(\frac{2n}{L} - 1\right)^2 \binom{L}{n} \left(\frac{1}{2}\right)^L - \mu^2$$

$$= \sum_{n=0}^{L} \left[\frac{4n^2}{L^2} - \frac{4n}{L} + 1\right] \left(\frac{L}{n}\right)\left(\frac{1}{2}\right)^L - \mu^2$$

$$= 1 - \mu^2 + \left(\frac{1}{2}\right)^{L-2} \left[\sum_{n=1}^{L} \frac{n^2}{L^2}\binom{L}{n} - \sum_{n=1}^{L} \frac{n}{L}\binom{L}{n}\right], \tag{39}$$

where the index has been shifted from $n = 0$ to $n = 1$ to account for the zero-value summand. By use of (8) the last summation becomes

$$\sum_{n=1}^{L} \frac{n}{L}\binom{L}{n} = \sum_{n=1}^{L} \frac{nL!}{Ln!(L-n)!}$$

$$= \sum_{n=1}^{L} \frac{(L-1)!}{(n-1)![L-1-(n-1)]!}$$

$$= \sum_{n=1}^{L} \binom{L-1}{n-1}$$

$$= \frac{(L-1)!}{(L-1)!} + \sum_{n=2}^{L} \binom{L-1}{n-1}$$

$$= 1 + \sum_{n=2}^{L} \binom{L-1}{n-1}. \tag{40}$$

From (19) and (8)

$$2^L = \sum_{n=0}^{L} \frac{L!}{n!(L-n)!}$$

$$= \frac{L!}{L!} + \sum_{n=1}^{L} \binom{L}{n}$$

$$= 1 + \sum_{n=1}^{L} \binom{L}{n} \tag{41}$$

When applied to the case $L = P - 1$ and $q = n + 1$, (41) becomes

$$2^{P-1} = 1 + \sum_{n=1}^{P-1} \binom{P-1}{n} = 1 + \sum_{q=2}^{P} \binom{P-1}{q-1}, \tag{42}$$

which, by an exchange of arbitrary parameters, can be rewritten as

$$\sum_{n=2}^{L} \binom{L-1}{n-1} = 2^{L-1} - 1. \tag{43}$$

Substitution of (43) into (40) gives

$$\sum_{n=1}^{L} \frac{n}{L} \binom{L}{n} = 2^{L-1}, \tag{44}$$

which, when substituted into (39), gives

$$\sigma^2 = \left(\frac{1}{2}\right)^{L-2} \sum_{n=1}^{L} \frac{n^2}{L^2} \binom{L}{n} - 1 - \mu^2$$

$$= \left(\frac{1}{2}\right)^{L-2} \sum_{n=1}^{L} \frac{n}{L} \frac{(L-1)!}{(n-1)!(L-n)!} - 1 - \mu^2$$

$$= \frac{1}{L} \left(\frac{1}{2}\right)^{J-1} \sum_{m=0}^{J} (M+1) \binom{J}{M} - 1 - \mu^2,$$

where $J = L - 1$ and $M = n - 1$. Then

$$\sigma^2 = \frac{1}{L} \left(\frac{1}{2}\right)^{J-1} \left[\sum_{M=1}^{J} M \binom{J}{M} + \sum_{M=0}^{J} \binom{J}{M} \right] - 1 - \mu^2. \tag{45}$$

From (44) and (19), (45) simplifies to

$$\sigma^2 = \frac{1}{L} \left(\frac{1}{2}\right)^{J-1} \left[J 2^{J-1} + 2^J \right] - 1 - \mu^2,$$

which further simplifies to

$$\sigma^2 = \frac{1}{L}(J+2) - 1 - \mu^2$$

$$= \frac{L+1}{L} - 1 - \mu^2$$

or finally

$$\boxed{\sigma^2 = \frac{1}{L} - \mu^2 \qquad = \frac{1}{L} - E(|\theta|)^2 .} \tag{46}$$

DETERMINATION OF THE EXPECTED VALUE FOR THE MAGNITUDE OF CORRELATION BETWEEN TWO GOLD-PAIR SEQUENCES

To obtain, for comparison, the distinguishing characteristics between purely random and PN Gold codes, the expected value and variance of the magnitude of crosscorrelation for a preferred pair of PN Gold sequences, over the various possible code-phase combinations, is also determined. Again, as in (10), where now $L = 2^N - 1$, the mean or expected value is

$$\mu_g = \sum_i |\theta_i| p_i . \tag{47}$$

But now

$$p_i = f_i/(2^N - 1) , \tag{48}$$

where f_i is the frequency or number of occurrences of a particular value of $|\theta_i|$ over the period. Since θ_i is a deterministic function for Gold pairs, the f_i can be uniquely determined.

Gold [5] has shown that the correlation for a Gold pair when N is odd can only be one of three specific values, namely,

$$\theta_1 = [-2^{(N+1)/2} - 1]/(2^N - 1) , \tag{49a}$$

$$\theta_2 = [2^{(N+1)/2} - 1]/(2^N - 1) , \tag{49b}$$

$$\theta_3 = -1/(2^N - 1) , \tag{49c}$$

with frequencies of occurrence

$$f_1 = 2^{N-2} - 2^{(N-3)/2}, \tag{50a}$$

$$f_2 = 2^{N-2} + 2^{(N-3)/2}, \tag{50b}$$

$$f_3 = 2^{N-1} - 1, \quad N \text{ odd}. \tag{50c}$$

Substitution of (48), (49), and (50) into (47) gives for N odd

$$\mu_g = \frac{[2^{(N+1)/2} + 1]}{(2^N - 1)^2} [2^{N-2} - 2^{(N-3)/2}]$$

$$+ \frac{[2^{(N+1)/2} + 1]}{(2^N - 1)^2} [2^{N-2} + 2^{(N-3)/2}] + \frac{2^{N-1} - 1}{(2^N - 1)^2}$$

$$\boxed{\mu_g = [2^{(3N-1)/2} - 2^{(N-1)/2} + 2^{N-1} - 1]/(2^N - 1)^2, \quad N \text{ odd}.} \tag{51}$$

Sherman [3] provides the distribution for N even, where $N = 6 + 4\lambda$ and $\lambda = 0, 1, 2, \ldots$. (Pairs of maximal length sequences with three-level crosscorrelation values do not exist for $N = 0, 4, 8, 12, \ldots$.) In this case the three correlation values and frequencies of occurrence are

$$\theta_1 = [-2^{(N+2)/2} - 1]/(2^N - 1), \tag{52a}$$

$$\theta_2 = [2^{(N+2)/2} - 1]/(2^N - 1), \tag{52b}$$

$$\theta_3 = -1/(2^N - 1), \tag{52c}$$

with

$$f_1 = 2^{N-3} - 2^{(N-4)/2}, \tag{53a}$$

$$f_2 = 2^{N-3} + 2^{(N-4)/2}, \tag{53b}$$

$$f_3 = 3(2^{N-2}) - 1, \quad N = 4\lambda; \quad \lambda = 0, 1, 2, 3, \ldots. \tag{53c}$$

Substitution of (48), (52), and (53) into (47) gives

$$\mu_g = \frac{[2^{N-3} - 2^{(N-4)/2}]}{(2^N - 1)^2} [2^{(N+2)/2} + 1]$$

$$+ \frac{[2^{N-3} + 2^{(N-4)/2}]}{(2^N - 1)^2} [2^{(N+2)/2} - 1] + \frac{3(2^{N-2}) - 1}{(2^N - 1)^2}$$

$$\boxed{\mu_g = [2^{(3N-2)/2} - 2^{(N-2)/2} + 3(2^{N-2}) - 1]/(2^N - 1)^2, \quad N = 6 + 4\lambda; \quad \lambda = 0, 1, 2, \ldots.} \tag{54}$$

DETERMINATION OF THE VARIANCE OF THE MAGNITUDE OF THE CORRELATION BETWEEN TWO GOLD-PAIR SEQUENCES

The variance of the magnitude of the correlation function for PN Gold pairs can be obtained in a similar manner. Thus, for N odd, by use of (38), (48), (49), and (50),

$$\sigma_g^2 = \sum_i \theta_i P_i - \mu_g^2$$

$$= \frac{[2^{(N+1)/2} + 1]^2}{(2^N - 1)^3} [2^{N-2} - 2^{(N-3)/2}]$$

$$+ \frac{[2^{(N+1)/2} - 1]^2}{(2^N - 1)^3} [2^{N-2} + 2^{(N-3)/2}] + \frac{2^{N-1} - 1}{(2^N - 1)^3} - \mu_g^2,$$

$$\boxed{\sigma_g^2 = \frac{2^{2N} - 2^N - 1}{(2^N - 1)^3} - \mu_g^2, \quad N \text{ odd}.} \tag{55}$$

For $N = 6 + 4\lambda$, $\lambda = 0, 1, 2, \ldots$, by use of (38), (48), (52), and (53),

$$\sigma_g^2 = \frac{[2^{(N+2)/2} + 1]^2}{(2^N - 1)^3} [2^{N-3} - 2^{(N-4)/2}]$$

$$+ \frac{[2^{(N+2)/2} - 1]^2}{(2^N - 1)^3} [2^{N-3} + 2^{(N-4)/2}] + \frac{3(2^{N-2}) - 1}{(2^N - 1)^3} - \mu_g^2$$

$$\boxed{\sigma_g^2 = \frac{2^{2N} - 2^N - 1}{(2^N - 1)^3} - \mu_g^2, \quad N = 6 + 4\lambda, \quad \lambda = 0, 1, 2, \ldots.} \tag{56}$$

The result is that (55) and (56) are of the same form.

THE CROSSCORRELATION AND OFF-PEAK AUTOCORRELATION UPPER BOUND FOR THE MEMBERS OF GOLD CODE FAMILIES

As previously stated, Gold [1,2] proved that the maximum magnitude of the *cross-correlation* which can occur for a preferred pair of maximal-length sequences is also the maximum crosscorrelation magnitude or bound that will be achieved for any combination of two members from the family of sequences known as *Gold-family* codes. A method of generating a Gold family of sequences is diagrammed in Fig. 1. Code A and code B are maximal-length linear sequences which constitute a preferred or Gold pair. Each has a period of length $2^N - 1$, for N-stage digital shift registers. A member C_i of the Gold family corresponding to codes A and B can be formed by the modulo-2 addition of code A with a particular phase of code B. The sequences formed in this manner belong to the

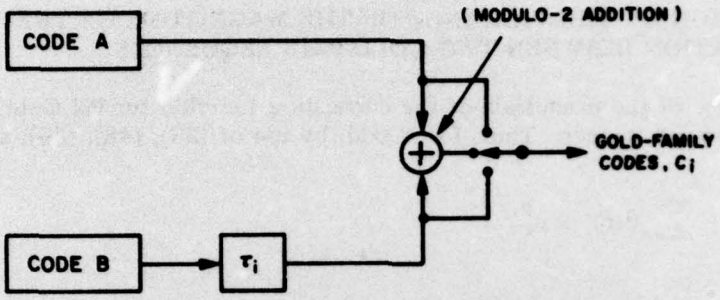


Fig. 1—A method of generating members of a Gold family of codes such that each member has a bounded crosscorrelation magnitude between itself and any other member within the family. τ_i is an integral number i of clock cycles of time delay for each member C_i of the family, where $i = 1, 2, \ldots, 2^N - 1$. Codes A and B are selected (Gold-Pair) N-stage shift-register-generated maximal-length linear sequences which are also members of the Gold code family.

nonmaximal class of codes; however, the two maximal-length sequences used to generate the other members of the family are themselves included in the family. Since there are $2^N - 1$ possible phases of code B, there are $2^N + 1$ members in the Gold family.

Golomb [6] gives the off-peak normalized *autocorrelation* values for a maximal-length linear sequence, such as used in generating a Gold code family (such as code A or code B), which are the same low value (the negative reciprocal of the sequence length), irrespective of the relative code phase. Thus the off-peak normalized autocorrelation magnitudes for either code A or code B are

$$|\theta| = 1/(2^N - 1). \tag{57}$$

The off-peak normalized autocorrelation magnitudes for the other members of the Gold family are not as ideal; however Gold has stated in a private communication that the off-peak autocorrelation values for all codes in a Gold family are bounded in magnitude and that this upper bound for any one family member is the same as the crosscorrelation magnitude bound for any two family members. This bound is known as the Gold bound. The largest crosscorrelation magnitude of the Gold pair used in generating the family can thus be used to characterize the crosscorrelation off-peak and autocorrelation bounds for the whole family of sequences.

The Gold bound for the normalized crosscorrelation and off-peak autocorrelation magnitudes over the full period for a Gold pair (or for any two members of the associated family of codes) is given by

$$\begin{aligned} |\theta| &< [2^{(N+1)/2} + 1]/(2^N - 1), \quad N \text{ odd}, \\ &< [2^{(N+2)/2} + 1]/(2^N - 1), \quad N \text{ even}. \end{aligned} \tag{58}$$

With N odd, this upper bound is a sharp bound in the sense that some relative phase shift of the pairs of sequences can be found that provides a magnitude of correlation which is

equal to the bound. With N even, however, there are some non-Gold-pair sequence combinations which yield maximum values for $|\theta|$ which are just slightly less than the bound indicated in (58).

A COMPARISON OF PSEUDONOISE GOLD-PAIR CODES AND INDEPENDENT RANDOM SEQUENCES

A FORTRAN computer program has been devised to evaluate the several expressions providing the mean, variance, and bounds, where applicable, for two random sequences and Gold-pair sequences of lengths $L = 2^N - 1$. The program listing is provided as Table 3. Table 4, Fig. 2, and Fig. 3 give the results as computed by the program. The program is based on equations (34), (36), (46), (51), (54), (55), (56), (57), and (58). The approximate relation given in (36), based on Stirling's approximation, is used when the length is greater than 10,000 in order to avoid excessive computation time.

The term Gold bound as used here is synonymous with bounds on the magnitudes of the normalized crosscorrelation of a Gold pair (or for the autocorrelation or crosscorrelation

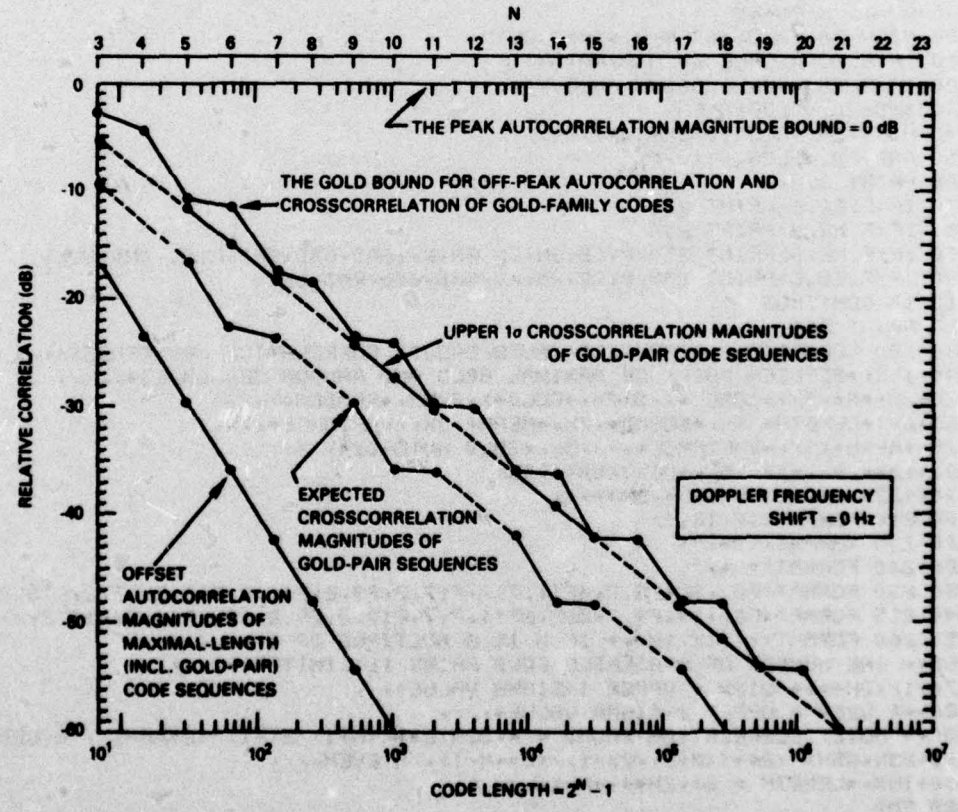


Fig. 2—The bounds and expected magnitudes of the normalized full-period autocorrelation and crosscorrelation of Gold family code sequences. (0 dB represents the largest possible correlation magnitude which occurs when there is either total agreement or disagreement among corresponding bits of the sequences.)

Table 3 — FORTRAN Program for Generating Table 4

```
00100 PROGRAM BCORR (OUTPUT)
00110 PRINT 200
00120 SQ2=SQRT(2.)
00130 DO 10 N=3,23
00140 G=N
00150 H=N/2
00160 H=H*2.
00170 F=N/4
00180 F=F*4.
00190 L=-1+2**N
00200 P=L
00210 E=0.5*(1.+N)
00220 T=2.**E
00230 IF(G.EQ.H)T=T*SQ2
00240 T=T+1.
00250 GB=T/P
00260 GBD=20.*ALOG10(GB)
00270 CALL AVTHETA(L,RM)
00280 RMD=20.*ALOG10(RM)
00290 RV=1./L-RM*RM
00300 U2SV=20.*ALOG10(RM+2.*SQRT(RV))
00310 IF(G.EQ.H)CALL EVEN(N,GM,GV)
00320 IF(G.NE.H)CALL ODD(N,GM,GV)
00330 GMD=20.*ALOG10(GM)
00340 U1SV=20.*ALOG10(GM+SQRT(GV))
00350 GAD=20.*ALOG10(1./P)
00360 PRINT 210,N
00370 IF(F.EQ.G)PRINT 230
00380 IF(F.NE.G)PRINT 240
00390 IF(F.NE.G)PRINT 250,P,GB,GM,GV,RM,RV,GAD,GBD,GMD,U1SV,RMD,U2SV
00400 IF(F.EQ.G)PRINT 255,P,GB,RM,RV,GAD,GBD,RMD,U2SV
00410 10 CONTINUE
00420 PRINT 260
00430 200 FORMAT(18X,*EXPECTED (AUTO/CROSS) CORRELATION MAGNITUDES*,/,
00440+15X,*BETWEEN PAIRS OF MAXIMAL GOLD AND RANDOM SEQUENCES*,///,
00450+2X,*N*,5X,*CODE *,,3(7X,*GOLD*),2(5X,*RANDOM*),/,
00460+6X,*LENGTH*,7X,*BOUND*,7X,*MEAN*,3X,*VARIANCE*,7X,
00470+*MEAN*,3X,*VARIANCE*,//,5X,*GOLD AUTO-DB*,7X,
00480+*DB*,9X,*DB*,5X,*U1SV(DB)*,7X,
00490+*DB*,3X,*U2SV(DB)*,2H**,/)
00500 210 FORMAT(1X,I2,^)
00510 230 FORMAT(1H*,^)
00520 240 FORMAT(* *,^)
00530 250 FORMAT(F8.,3X,F9.7,4F11.7,/,F17.2,F9.2,F11.2,F13.2,F9.2,F13.2,/)
00540 255 FORMAT(F8.,3X,F9.7,22X,2F11.7,/,F17.2,F9.2,22X,F11.2,F13.2,/)
00550 260 FORMAT(//,1X,1H*,* IF N IS A MULTIPLE OF 4,*,
00560+* THE NUMBER OF AVAILABLE GOLD PAIRS IS LIMITED.*,//,
00570+1X,2H**,* U1SV = UPPER 1-SIGMA VALUE*,
00580+*; U2SV = UPPER 2-SIGMA VALUE*,//,
00590+* NOTE: CORRELATION BOUND = *,32H(2**((N+1)/2)+1)/(2**N-1), N ODD,/,
00600+25X,35H= (2**((N+2)/2)+1)/(2**N-1), N EVEN,//,
00610+18X,*LENGTH = 2*,2H**,*N-1*,///)
00620 END
00630C
```

Table 3 (Continued) — FORTRAN for Generating Table 4

```
00640C
00650 SUBROUTINE AVTHETA(L,RM)
00660 J=L   $   RM=L/2   $   K=RM+2.
00670 IF(K.EQ.L)J=J+1
00680 IF(L.LT.10000)GO TO 5
00690 RM=SQRT(0.6366197723657495/(J-1))
00700 GO TO 20
00710 5 CONTINUE
00720 K=0
00730 J=(J-1)/2
00740 RM=1.
00750 DO 10 I=1,J
00760 X=K=K+1   $   Y=K=K+1
00770 RM=RM*X/Y
00780 10 CONTINUE
00790 20 CONTINUE
00800 RETURN
00810 END
00820C
00830C
00840 SUBROUTINE ODD(N,GM,GV)
00850 F1=2.**(-N)
00860 F2=1.-F1
00870 F3=2.**(-(1+N)/2)
00880 F4=F3-2.**(-(3*N+1)/2)+2.**(-1-N)
00890+-2.**(-2*N)
00900 GM=(F4/F2)/F2
00910 F5=2.**(-(N-1)/2)
00920 F6=2.**(-(N+3)/2)
00930 GV=(F5+F1)**2*(0.25-F6)
00940 GV=GV+(F5-F1)**2*(0.25+F6)
00950 GV=GV+2.**(-2*N-1)-2.**(-3*N)
00960 GV=((GV/F2)/F2)/F2-GM*GM
00970 RETURN
00980 END
00990C
01000C
01010 SUBROUTINE EVEN(N,GM,GV)
01020 F1=2.**(-N)
01030 F2=1.-F1
01040 F3=2.**(-(2+N)/2)
01050 F4=F3-2.**(-(3*N+2)/2)+3.*2.**(-2-N)
01060+-2.**(-2*N)
01070 GM=(F4/F2)/F2
01080 F5=2.**(-(N-2)/2)
01090 F6=2.**(-(N+4)/2)
01100 GV=(F5+F1)**2*(0.125-F6)
01110 GV=GV+(F5-F1)**2*(0.125+F6)
01120 GV=GV+3.*2.**(-2*N-2)-2.**(-3*N)
01130 GV=((GV/F2)/F2)/F2-GM*GM
01140 RETURN
01150 END
```

Table 4 — Expected (Auto/Cross) Correlation Magnitudes Between Pairs of Maximal Gold and Random Sequences

N	CODE LENGTH	GOLD BOUND	GOLD MEAN	GOLD VARIANCE	RANDOM MEAN	RANDOM VARIANCE
	GOLD AUTO-DB	DB	DB	U1SV(DB)	DB	U2SV(DB)••
3	7	.7142857	.3469388	.0399833	.3125000	.0452009
	-16.90	-2.92	-9.19	-5.24	-10.10	-2.64
4•	15	.6000000			.2094727	.0227879
	-23.52	-4.44			-13.58	-5.93
5	31	.2903226	.1446410	.0123441	.1444644	.0113861
	-29.83	-10.74	-16.79	-11.84	-16.80	-8.92
6	63	.2698413	.0753338	.0104458	.1009237	.0056874
	-35.99	-11.38	-22.46	-15.01	-19.92	-11.98
7	127	.1338583	.0668981	.0034602	.0709403	.0028415
	-42.08	-17.47	-23.49	-18.01	-22.98	-15.01
8•	255	.1294118			.0500145	.0014201
	-48.13	-17.76			-26.02	-18.04
9	511	.0645793	.0322877	.0009183	.0353136	.0007099
	-54.17	-23.80	-29.82	-24.07	-29.04	-21.05
10	1023	.0635386	.0163732	.0007104	.0249522	.0003549
	-60.20	-23.94	-35.72	-27.33	-32.06	-24.06
11	2047	.0317538	.0158768	.0002367	.0176374	.0001774
	-66.22	-29.96	-35.98	-30.10	-35.07	-27.08
12•	4095	.0315018			.0124692	.0000887
	-72.25	-30.03			-38.08	-30.09
13	8191	.0157490	.0078745	.0000601	.0088163	.0000444
	-78.27	-36.05	-42.08	-36.12	-41.09	-33.10
14	16383	.0156870	.0039523	.0000454	.0062339	.0000222
	-84.29	-36.09	-48.06	-39.42	-44.10	-36.11
15	32767	.0078433	.0039216	.0000151	.0044079	.0000111
	-90.31	-42.11	-48.13	-42.14	-47.12	-39.12
16•	65535	.0078279			.0031168	.0000055
	-96.33	-42.13			-50.13	-42.13
17	131071	.0039139	.0019570	.0000038	.0022039	.0000028
	-102.35	-48.15	-54.17	-48.16	-53.14	-45.14
18	262143	.0039101	.0009794	.0000029	.0015584	.0000014
	-108.37	-48.16	-60.18	-51.47	-56.15	-48.15
19	524287	.0019550	.0009775	.0000010	.0011019	.0000007
	-114.39	-54.18	-60.20	-54.19	-59.16	-51.16
20•	1048575	.0019541			.0007792	.0000003
	-120.41	-54.18			-62.17	-54.17
21	2097151	.0009770	.0004885	.0000002	.0005510	.0000002
	-126.43	-60.20	-66.22	-60.21	-65.18	-57.18
22	4194303	.0009768	.0002443	.0000002	.0003896	.0000001
	-132.45	-60.20	-72.24	-63.52	-68.19	-60.19
23	8388607	.0004884	.0002442	.0000001	.0002755	.0000000
	-138.47	-66.22	-72.25	-66.23	-71.20	-63.20

• IF N IS A MULTIPLE OF 4, THE NUMBER OF AVAILABLE GOLD PAIRS IS LIMITED.

•• U1SV = UPPER 1-SIGMA VALUE; U2SV = UPPER 2-SIGMA VALUE

NOTE: CORRELATION BOUND = $(2^{\bullet\bullet}((N+1)/2)+1)/(2^{\bullet\bullet}N-1)$, N ODD
= $(2^{\bullet\bullet}((N+2)/2)+1)/(2^{\bullet\bullet}N-1)$, N EVEN

LENGTH = $2^{\bullet\bullet}N-1$

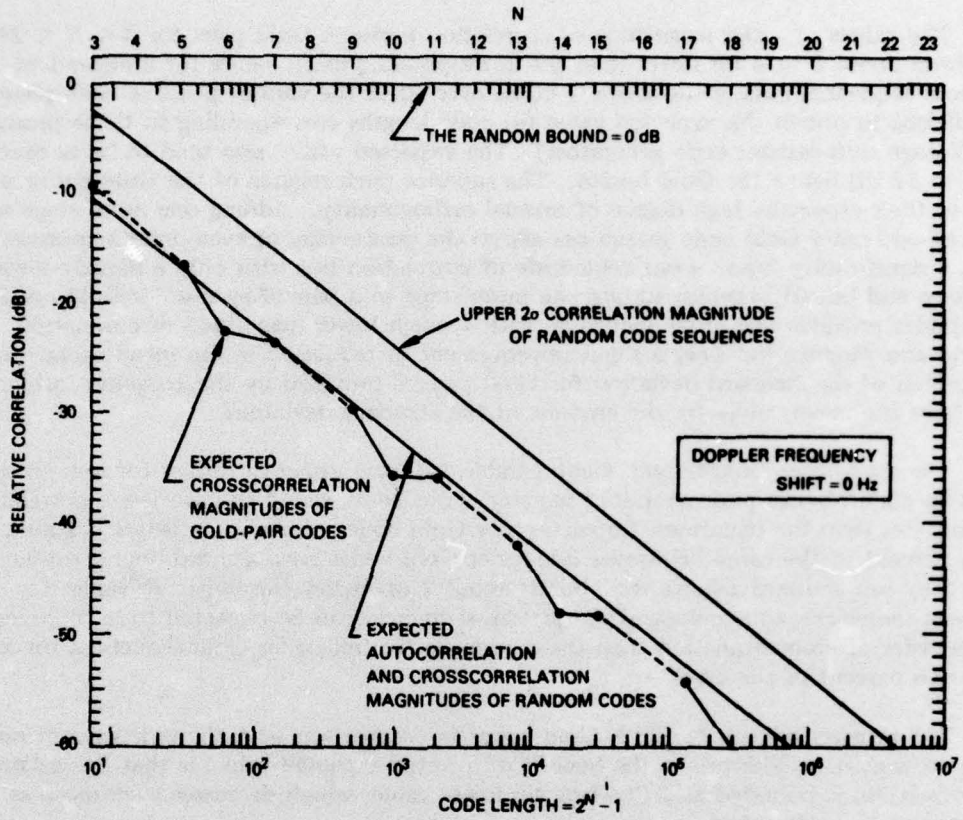


Fig. 3 — The bound and expected distribution of the normalized correlation of independent random sequences. (The expected crosscorrelation magnitudes of Gold-Pair codes are shown for comparison.)

between any two members of a Gold family of codes). The upper 2σ values are equal to the mean value plus twice the standard deviation, or the square root of the variance. In the case of random sequences with Gaussian distributions, the upper 2σ values are exceeded with a probability of only 0.025.

Table 4, Fig. 2, and Fig. 3 permit a comparison between the expected properties of the magnitude of crosscorrelation between PN Gold pairs and pairs of purely random sequences in relation to the bound determined by Gold given in (58). Several maximal-length sequences of period $L = 2^N - 1$ are examined, where N is the number of stages in each of the two binary shift-register code generators. The autocorrelation of independent random codes is the same as their crosscorrelation. Although the off-peak autocorrelation magnitudes of Gold-family codes are limited by the Gold bound just as the crosscorrelation magnitudes are, the off-peak autocorrelation magnitudes of all maximal-length sequences of the same length are considerably lower. The 0-dB bound for the magnitude of the autocorrelation or crosscorrelation of random codes occurs whenever corresponding bits in the two sequences happen to either all agree or all disagree.

The values of mean magnitude of correlation between Gold pairs for $3 < N < 24$ are from about 0 to 4 dB lower than the corresponding mean values for independent random sequences (where the mean is taken over all of the various possible code phase conditions to obtain the expected value for code lengths corresponding to those produced by N-stage shift-register code generators). The expected values also tend to be as much as 6 to 12 dB below the Gold bound. The superior performance of the Gold codes is due to their especially high degree of mutual orthogonality. Adding one more stage to a pair of odd-order Gold code generators allows the production of even-order sequences with a significantly lower mean magnitude of correlation but with only a slightly lower variance and bound, whereas adding one more stage to a pair of even-order Gold code generators provides odd-order sequences with a much lower magnitude of correlation bound and variance but only a slight improvement or reduction in the mean value. An indication of the standard deviation for Gold pairs is provided by the 1σ values, which lie above the mean values by the amount of the standard deviation.

The even-order Gold bound is comparable with the upper 2σ values for independent random codes; hence purely random sequences can be expected to have lower correlation magnitudes than the maximum for even-order Gold codes of the same length for about 97.5 percent of the cases. However odd-order Gold codes have a sharp bound (meaning that they can at times achieve the bound) about 2 dB below the upper 2σ values for random sequences; thus independent random sequences can be expected to have larger magnitudes of crosscorrelation than the maximum for odd-order Gold sequences for more than 2.5 percent of the cases.

The primary advantage of PN Gold codes in comparison with the independent random sequences, in addition to the benefit of a lower expected value, is that the magnitude of correlation is bounded at a significantly lower value, which decreases even more as sequences are made longer.

SUMMARY

The magnitude of correlation of purely random sequences has been evaluated to provide a fundamental point of reference needed for characterizing the relative performance properties of pseudonoise sequences. Expressions for the mean or expected value and the variance for the magnitude of the full-period correlation between independent random sequences and also PN Gold pairs have been determined for code lengths up through those corresponding to the period of maximal-length sequences from 23-stage binary shift-register code generators.

The comparison of the crosscorrelation characteristics of independent random sequences and PN Gold pairs reveals certain advantages of Gold pairs due to their inherent mutual orthogonality.

The importance of choosing longer sequences whenever possible is clearly indicated in all cases; for not only is the expected magnitude of autocorrelation and crosscorrelation decreased thereby, but the variances are also lowered. Longer sequences thus provide better correlation performance, whether they be purely random or pseudonoise Gold codes, achieved by the use of more stages in the binary shift-register code generators.

The analysis of the magnitude of correlation for random sequences provided here is useful for evaluating the expected performance of signal correlation detectors which function on the basis of the magnitude of correlation with a reference sequence while they are operating on noise-only input.

ACKNOWLEDGMENTS

The authors gratefully acknowledge and express appreciation for the helpful comments of Mr. Charles F. White, Dr. Robert Gold, and Mr. William E. Leavitt.

REFERENCES

1. R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE NAECON Proceedings, National Aerospace Electronics Conference, Dayton, Ohio, p. 173, 1966.
2. R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing," IEEE Trans. on Information Theory *IT-13* (No. 4), 619-621, Oct. 1967.
3. R.J. Sherman, "Generalized Correlation Properties of Gold Codes," Technical Memorandum 230, Philco-Ford Corp., Western Development Laboratories, Palo Alto, Calif. 94303, Jan. 1974.
4. "GPS/TRIDENT Code Design," Vol. I, Report STI/GPS-051, Stanford Telecommunications, Inc., Mountainview, Calif. 94043, Aug. 6, 1975 (prepared for SAMSO, Los Angeles, under contract F04701-74-C-0310).
5. R. Gold, "Maximal Recursive Sequences with 3-Valued Recursive Cross-Correlation Functions," IEEE Trans. on Information Theory *IT-14* (No. 1), 154-156, Jan. 1968.
6. S.W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967.