Pseudo-random sequences and arrays

Article *in* Proceedings of the IEEE · January 1977

DOI: 10.1109/PROC.1976.10411 · Source: IEEE Xplore

2 authors, including:

N. J. A. Sloane
The OEIS Foundation Inc.
456 PUBLICATIONS **52,261** CITATIONS

rent rotating arcs," *Inst. Elec. Eng. Int. Conference on Gas Discharges*, pp. 534-538, 1974.
[54] A. E. Guile, "Model of emitting sites and erosion on nonrefractory arc cathodes with relatively thick oxide films," *Proc. Inst. Elec. Eng.*, vol. 121, pp. 1594-1598, 1974.
[55] J. E. Harry, "The measurement of the erosion rate at the electrodes of an arc rotated by a transverse magnetic field," *J. Appl. Phys.*, vol. 40, pp. 265-270, 1969.
[56] A. E. Guile and J. G. J. Sloot, "Sudden transitions in velocity of magnetically driven arcs," in *Conf. Rec., IEE Int. Conf. on Gas Discharges*, pp. 544-548, 1974.
[57] K. Taylor, "British Railways' experience with pantographs for high-speed running," *J. Inst. Mech. Eng. (Railway Division)*, vol. 2, pt. 4, pp. 349-373, 1971.
[58] A. E. Guile, V. W. Adams, W. T. Lord, and K. A. Naylor, "High-current arcs in transverse magnetic fields in air at atmospheric pressure," *Proc. Inst. Elec. Eng.*, vol. 116, pp. 645-652, 1969.
[59] A. E. Guile and A. H. Hitchcock, "Time variation in copper cathode erosion rate for long duration arcs," *J. Phys. D.*, vol. 8, pp. 427-433, 1975.
[60] C. W. Kimblin, "Anode phenomena in vacuum and atmospheric pressure arcs," *IEEE Trans. Plasma Science*, vol. PS-2, pp. 310-319, 1974.
[61] A. E. Guile and A. H. Hitchcock, "The effect of rotating arc velocity on copper cathode erosion," *J. Phys. D*, vol. 7, pp. 597-606, 1974.
[62] H. Edels, "The arc discharge, Pt. 2, Interruption and reignition," *Proc. VI Yugoslav Symposium and Summer School on the Physics of Ionized Gases* (Miljevac by Split, Yugoslavia), pp. 419-439, 1972.
[63] J. F. Perkins, "Dielectric recovery and interruption variability of air arcs at atmospheric pressure," *IEEE Trans. Power App. Syst.*, vol. PAS-93, pp. 281-288, 1974.
[64] J. Clark, "Electromagnetic interference shielding," *Electron*, No. 51, pp. 80, 85, 87, and 89, May 1974.
[65] D. Klapas, "Anode spot transition phenomena in low current copper vacuum arcs," Ph.D. thesis, Liverpool University, 1973.
[66] T. Takakura, K. Baba, K. Nunogaki, and H. Mitani, "Radiation of plasma noise from arc discharge," *J. Appl. Phys.*, vol. 26, pp. 185-189, 1955.
[67] M. I. Skolnik and H. R. Puckett Jr., "Relaxation oscillations and noise from low-current arc discharges," *J. Appl. Phys.*, vol. 26, pp. 74-79, 1955.
[68] G. R. Jordan, B. Bowman, and D. Wakelam, "Electrical and photographic measurements of high-power arcs," *J. Phys. D:* vol. 3, pp. 1089-1099, 1970.

Pseudo-Random Sequences and Arrays

F. JESSIE MacWILLIAMS AND NEIL J. A. SLOANE, MEMBER, IEEE

Abstract—**Binary sequences of length $n = 2^m - 1$ whose autocorrelation function is either 1 or $-1/n$ have been known for a long time, and are called pseudo-random (or PN) sequences, or maximal-length shift-register sequences. Two-dimensional arrays of area $n = 2^{lm} - 1$ with the same property have recently been found by several authors. This paper gives a simple description of such sequences and arrays and their many nice properties.**

I. Introduction

PSEUDO-RANDOM SEQUENCES (which are also called pseudo-noise (PN) sequences, maximal-length shift-register sequences, or m-sequences) are certain binary sequences of length $n = 2^m - 1$ (the construction is given in Section II). They have many useful properties, one of which is that their periodic autocorrelation function is given by

$$\rho(0) = 1 \qquad \rho(i) = -\frac{1}{n}, \qquad \text{for } 1 \leqslant i \leqslant n-1 \tag{1}$$

(see Section II-D and especially Fig. 9). These sequences have been known for a long time, are used in range-finding, scrambling, fault detection, modulation, synchronizing, etc., and a considerable body of literature exists. See for example [2], [13], [16], [19], [20], [24], [27], [31], [36], [43b], [55], [58], [67a], [68], [72], [74], [75], and especially Golomb [28], [29], Kautz [42], Selmer [60], Zierler [76], [77], and [44, ch. 14].

Nevertheless they are not as widely known as they should be, especially outside of the area of communication theory—see [61], [62], [66]—and there does not seem to exist a simple, comprehensive account of their properties. The reader will find such an account in Section II of this paper.

Recently, several applications ([37], [38], [43], [59]) have called for two-dimensional arrays whose two-dimensional autocorrelation function should satisfy $\rho(0, 0) = 1$, $\rho(i, j)$ small for $(i, j) \neq (0, 0)$. We shall see in Section III that it is very easy to use pseudo-random sequences to obtain $n_1 \times n_2$ arrays with

$$\rho(0, 0) = 1 \qquad \rho(i, j) = -\frac{1}{n}, \qquad \text{for } 0 \leqslant i < n_1, \quad 0 \leqslant j < n_2, \quad (i, j) \neq (0, 0) \tag{2}$$

where $n = 2^m - 1 = n_1 n_2$, provided n_1 and n_2 are relatively prime. The construction is a standard one in studying product codes (see [26], [10]). For earlier work on two-dimensional arrays see Reed and Stewart [54], Spann [63], Gordon [30], Calabro and Wolf [12], Nomura *et al.* [48]-[51], Ikai and Kojima [40], and Imai [41]. The construction given in Section III does not seem to be mentioned in these papers, although it can be shown ([44, ch. 18]) to be equivalent to a special case of the constructions given by Nomura *et al.*

Manuscript received June 1, 1976; revised August 19, 1976.
The authors are with Bell Laboratories, Murray Hill, NJ 07974.

One of the problems considered in these papers is the construction of arrays with the *window property*. This means that if a window of prescribed size, say $k_1 \times k_2$, is slid over the array, each of the $2^{k_1 k_2} - 1$ possible nonzero $k_1 \times k_2$ arrays is seen through the window exactly once. (To avoid trouble at the edges, either several copies of the array are placed side by side, or alternatively the array is written on a torus.) We shall see in Section III-B and the Appendix that our arrays have the window property.

It is straightforward to generalize the construction given in Section III to obtain three and higher dimensional arrays with flat autocorrelation function; we leave the details to the reader.

To find sequences (and arrays) whose *aperiodic* autocorrelation function is flat is a different problem altogether—see Turyn [69] and Lindner [43c].

The outline of this paper is as follows. Section II describes pseudo-random arrays and their many nice properties and connections with other parts of mathematics. A particularly useful property is Property XIII, in Section II-K, which says that the pseudo-random sequences of length $2^m - 1$, together with the zero sequence, are isomorphic to a field with 2^m elements. Section III describes pseudo-random arrays and properties. So far everything has been binary, but in Section IV we describe pseudo-random sequences and arrays with elements taken from an alphabet of q symbols, where q is a prime power. A kind of generalized autocorrelation function of pseudo-random arrays, called the transmission function, is studied in Section V. A short summary appears in Section VI.

II. Pseudo-Random Sequences

A. The Shift Register

To construct a pseudo-random sequence of length $n = 2^m - 1$, one needs a primitive polynomial $h(x)$ of degree m. This term is defined below; for the moment we take

$$h(x) = x^4 + x + 1 \tag{3}$$

as an example of degree $m = 4$. This polynomial specifies a *feedback shift register* as shown in Fig. 1. In general this is a shift register consisting of m little boxes, representing memory elements or flip-flops, each containing a 0 or 1. At each time unit the contents of the boxes are shifted one place to the right, and the boxes corresponding to the terms in $h(x)$ are added and fed into the left-hand box. The sum is calculated mod 2, so $\rightarrow\oplus\rightarrow$ in the figures represents a mod-2 adder or EXCLUSIVE-OR gate, defined by $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$.

In the above example, if the register contains $a_{i+3}, a_{i+2}, a_{i+1}, a_i$ at time i, then at time $i + 1$ it contains

$$a_{i+4} = a_{i+1} + a_i, \quad a_{i+3}, a_{i+2}, a_{i+1}$$

as shown in Fig. 2. In other words, this feedback shift register generates an infinite sequence $a_0 a_1 a_2 \cdots a_i \cdots$ which satisfies the recurrence

$$a_{i+4} = a_{i+1} + a_i, \quad i = 0, 1, \cdots, \tag{4}$$

where + denotes addition mod 2. The shift register needs to be started up, so we must specify the initial values $a_0, a_1, \cdots, a_{m-1}$.

Here is a more complicated example. When $m = 8$, we take

$$h(x) = x^8 + x^6 + x^5 + x + 1 \tag{5}$$

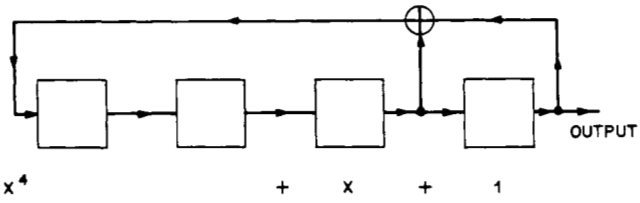


Fig. 1. Feedback shift register corresponding to $x^4 + x + 1$.

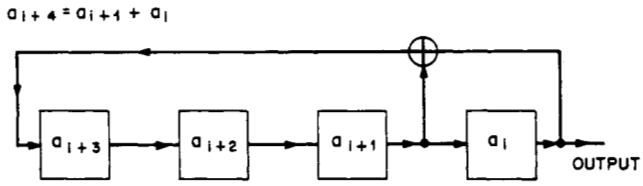


Fig. 2. The shift register specifies a recurrence relation.

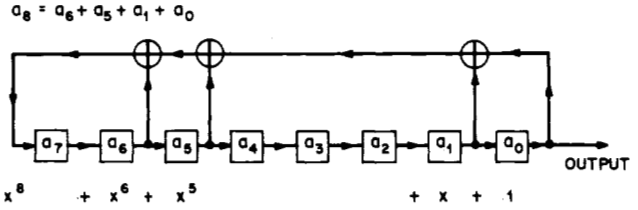


Fig. 3. Feedback shift register corresponding to $x^8 + x^6 + x^5 + x + 1$.

the shift register is shown in Fig. 3, and the output sequence satisfies the recurrence

$$a_{i+8} = a_{i+6} + a_{i+5} + a_{i+1} + a_i, \quad i = 0, 1, \cdots, \tag{6}$$

with initial values $a_0, a_1, \cdots, a_7$.

B. Pseudo-Random Sequences

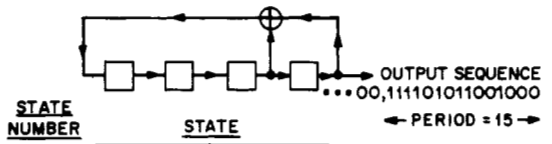
Since each of the m boxes contains a 0 or 1, there are 2^m possible states for the shift register. Thus the sequence $a_0 a_1 a_2 \cdots$ must be periodic. But the zero state $00 \cdots 0$ can't occur unless the sequence is all zeros. So the maximum possible period is $2^m - 1$.

We can now define a *primitive* polynomial $h(x)$. This is one for which $a_0 a_1 a_2 \cdots$ has period $2^m - 1$ (for some starting state). For example, Fig. 4 shows the successive states and output sequence of Fig. 1 if the initial state is 1000. (Note that the output sequence is the same as the right-hand column of the list of states. The output is equal to the parity of the binary number corresponding to the state.) Since the output sequence has period $15 = 2^4 - 1$, $x^4 + x + 1$ *is* a primitive polynomial. Similarly the output of Fig. 3 has period $255 = 2^8 - 1$.

We ask the reader to accept this fact: there exist primitive polynomials of degree m for every m. (The rather complicated proof can be found for example in [8] or [44, ch. 4].) Fig. 5 gives a table for $m \leqslant 40$, sufficient to generate sequences of period up to $2^{40} - 1 \approx 10^{12}$, enough for most purposes. Fig. 5 is taken from Stahnke [64], who gives a table for $m \leqslant 168$. Primitive polynomials of much higher degree have been found by Zierler and Brillhart [78].

It follows that if $h(x)$ is a primitive polynomial of degree m, the shift register goes through all $2^m - 1$ distinct nonzero states before repeating, and produces an output sequence

$$a_0 a_1 a_2 \cdots \tag{7}$$



STATE NUMBER	STATE			
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	1	0	0	1
4	1	1	0	0
5	0	1	1	0
6	1	0	1	1
7	0	1	0	1
8	1	0	1	0
9	1	1	0	1
10	1	1	1	0
11	1	1	1	1
12	0	1	1	1
13	0	0	1	1
14	0	0	0	1
15 = 0	1	0	0	0
16 = 1	0	1	0	0

(REPEATS)

Fig. 4. Successive states and output sequence from shift register.

deg m	$h(x)$	deg m	$h(x)$
1	$x+1$	21	$x^{21}+x^2+1$
2	x^2+x+1	22	$x^{22}+x+1$
3	x^3+x+1	23	$x^{23}+x^5+1$
4	x^4+x+1	24	$x^{24}+x^4+x^3+x+1$
5	x^5+x^2+1	25	$x^{25}+x^3+1$
6	x^6+x+1	26	$x^{26}+x^8+x^7+x+1$
7	x^7+x+1	27	$x^{27}+x^8+x^7+x+1$
8	$x^8+x^6+x^5+x+1$	28	$x^{28}+x^3+1$
9	x^9+x^4+1	29	$x^{29}+x^2+1$
10	$x^{10}+x^3+1$	30	$x^{30}+x^{16}+x^{15}+x+1$
11	$x^{11}+x^2+1$	31	$x^{31}+x^3+1$
12	$x^{12}+x^7+x^4+x^3+1$	32	$x^{32}+x^{28}+x^{27}+x+1$
13	$x^{13}+x^4+x^3+x+1$	33	$x^{33}+x^{13}+1$
14	$x^{14}+x^{12}+x^{11}+x+1$	34	$x^{34}+x^{15}+x^{14}+x+1$
15	$x^{15}+x+1$	35	$x^{35}+x^2+1$
16	$x^{16}+x^5+x^3+x^2+1$	36	$x^{36}+x^{11}+1$
17	$x^{17}+x^3+1$	37	$x^{37}+x^{12}+x^{10}+x^2+1$
18	$x^{18}+x^7+1$	38	$x^{38}+x^6+x^5+x+1$
19	$x^{19}+x^6+x^5+x+1$	39	$x^{39}+x^4+1$
20	$x^{20}+x^3+1$	40	$x^{40}+x^{21}+x^{19}+x^2+1$

Fig. 5. Primitive polynomials.

of period $2^m - 1$. We call any segment

$$a_i a_{i+1} \cdots a_{i+2m-2} \tag{8}$$

of length $2^m - 1$ a *pseudo-random sequence*. There are $2^m - 1$ different pseudo-random sequences [taking $i = 0, 1, \cdots, 2^m - 2$ in (8)]; those corresponding to Fig. 4 are shown in Fig. 6.

Note that if a different nonzero initial state is used, this is still one of the states the shift register goes through, and the new output sequence is just a shift of (7), namely $a_r a_{r+1} a_{r+2} \cdots$ for some r. Therefore the same set of pseudo-random sequences is obtained from any nonzero starting state. (Of course changing $h(x)$ will give a different set of sequences. For example using $x^4 + x^3 + 1$ instead of $x^4 + x + 1$ reverses the sequences in Fig. 6.)

```
0 0 0 1 0 0 1 1 0 1 0 1 1 1 1
0 0 1 0 0 1 1 0 1 0 1 1 1 1 0
0 1 0 0 1 1 0 1 0 1 1 1 1 0 0
1 0 0 1 1 0 1 0 1 1 1 1 0 0 0
0 0 1 1 0 1 0 1 1 1 1 0 0 0 1
0 1 1 0 1 0 1 1 1 1 0 0 0 1 0
1 1 0 1 0 1 1 1 1 0 0 0 1 0 0
1 0 1 0 1 1 1 1 0 0 0 1 0 0 1
0 1 0 1 1 1 1 0 0 0 1 0 0 1 1
1 0 1 1 1 1 0 0 0 1 0 0 1 1 0
0 1 1 1 1 0 0 0 1 0 0 1 1 0 1
1 1 1 1 0 0 0 1 0 0 1 1 0 1 0
1 1 1 0 0 0 1 0 0 1 1 0 1 0 1
1 1 0 0 0 1 0 0 1 1 0 1 0 1 1
1 0 0 0 1 0 0 1 1 0 1 0 1 1 1
```

Fig. 6. The 15 pseudo-random sequences obtained from Fig. 4.

```
  LENGTH =    3

011

  LENGTH =    7

0010111

  LENGTH =   15

000100110101111

  LENGTH =   31

00001001011001111100011011101O1

  LENGTH =   63

000001000011000101001111010003111001001011011101100
11010101111111

  LENGTH =  127

00000010000011000010100011111001000101100111010100
11111010CC0111C001001001101101011011110110001101001
01110111001100101010111111

  LENGTH =  255

00000001011100011101111000101100110110000111100111
00000101011111111001011110100101000011011101101111
01011101000001100101010100011010110001100000100101
10110101C011010011111101110C1100111101100100010000
00011100100100110001001110101011010001000101001000
11111
```

Fig. 7. Examples of pseudo-random sequences.

Fig. 7 gives one pseudo-random sequence of length $2^m - 1$ for each m between 2 and 8, obtained from the primitive polynomials of Fig. 5 with initial state $100 \cdots 0$.

Remark

It is possible to attain period 2^m (rather than $2^m - 1$) using a nonlinear shift register. The corresponding output sequence is called a *de Bruijn cycle* ([11a], [19a], [19b], [29], [43a]).

C. Properties of Pseudo-Random Sequences

Let $h(x)$ be a fixed primitive polynomial of degree m, and let δ_m be the set consisting of the pseudo-random sequences obtained from $h(x)$, together with the sequence of $2^m - 1$ zeros (denoted by **0**). These pseudo-random sequences are the $2^m - 1$ different segments

$$a_i a_{i+1} \cdots a_{i+2m-2}, \qquad i = 0, 1, \cdots, 2^m - 2$$

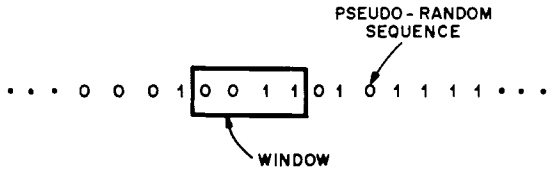


Fig. 8. The window property: Every nonzero 4-tuple is seen once.

of length $2^m - 1$ from the output of the shift register specified by $h(x)$. For example, δ_4 consists of **0** and the rows of Fig. 6.

We proceed to give the properties of these sequences. Properties I and II follow from the preceding discussion.

Property I—The Shift Property: If $b = b_0 b_1 \cdots b_{2^m-2}$ is any pseudo-random sequence in δ_m, then any cyclic shift of b, say

$$b_j b_{j+1} \cdots b_{2^m-2} b_0 \cdots b_{j-1}$$

is also in δ_m.

Property II—The Recurrence: Suppose $h(x) = \sum_{i=0}^{m} h_i x^i$, with $h_0 = h_m = 1$, $h_i = 0$ or 1 for $0 < i < m$. Any pseudo-random sequence $b \in \delta_m$ satisfies the recurrence

$$b_{i+m} = h_{m-1} b_{i+m-1} + h_{m-2} b_{i+m-2} + \cdots + h_1 b_{i+1} + b_i \quad (9)$$

for $i = 0, 1, \cdots$. (This generalizes (4) and (6).) Conversely any solution of (9) is in δ_m. Using all $2^m - 1$ distinct nonzero initial values $b_0, \cdots, b_{m-1}$ in (9) we obtain the $2^m - 1$ pseudo-random sequences. There are m linearly independent solutions to (9), hence m linearly independent sequences in δ_m.

Property III—The Window Property: If a window of width m is slid along a pseudo-random sequence in δ_m, each of the $2^m - 1$ nonzero binary m-tuples is seen exactly once—see Fig. 8 for the case $m = 4$. (This follows from the fact that $h(x)$ is a primitive polynomial.)

To avoid difficulties at the ends, either imagine three copies of the sequence are placed next to each other, or alternatively that the sequence is written in a circle.

Property IV—Half 0's and Half 1's: Any pseudo-random sequence in δ_m contains 2^{m-1} 1's and $2^{m-1} - 1$ 0's. (This is because there are 2^{m-1} odd numbers between 1 and $2^m - 1$, with binary representation ending in 1, and $2^{m-1} - 1$ even numbers in the same range, with binary representation ending in 0. The state of the shift register runs through these numbers, and the output is equal to the parity of the state—see Fig. 4.)

Property V—The Addition Property: The sum of two sequences in δ_m (formed componentwise, modulo 2, without carries) is another sequence in δ_m. (For the sum of two solutions to (9) is another solution.) E.g. the sum of the first two sequences in Fig. 6 is the fifth sequence.

Property VI—The Shift-and-Add Property: The sum of a pseudo-random sequence and a cyclic shift of itself is another pseudo-random sequence. (From Properties I and V.)

D. Autocorrelation Function

We come now to the most important property, the autocorrelation function. The *autocorrelation function* $\rho(i)$ of a real (or complex) sequence $s_0 s_1 \cdots s_{n-1}$ of length n is defined by

$$\rho(i) = \frac{1}{n} \sum_{j=0}^{n-1} s_j \bar{s}_{i+j}, \quad i = 0, \pm 1, \pm 2, \cdots \quad (10)$$

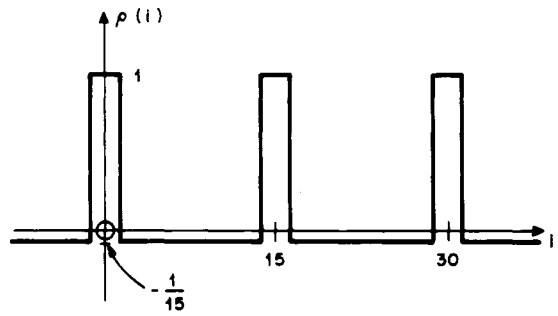


Fig. 9. Autocorrelation function of a pseudo-random sequence.

where subscripts are reduced mod n if they exceed $n - 1$, and the bar denotes complex conjugation. This is a periodic function: $\rho(i) = \rho(i + n)$. The autocorrelation function of a binary sequence $a_0 a_1 \cdots a_{n-1}$ is then defined to be equal to the autocorrelation function of the real sequence $(-1)^{a_0}, (-1)^{a_1}, \cdots, (-1)^{a_{n-1}}$ obtained by replacing 1's by -1's and 0's by $+1$'s. Thus

$$\rho(i) = \frac{1}{n} \sum_{j=0}^{n-1} (-1)^{a_j + a_{i+j}}.$$

Alternatively, let A be the number of places where $a_0 \cdots a_{n-1}$ and the cyclic shift $a_i a_{i+1} \cdots a_{i-1}$ agree, and D the number of places where they disagree (so $A + D = n$). Then

$$\rho(i) = \frac{A - D}{n}. \quad (11)$$

For example, the pseudo-random sequence given in the first row of Fig. 6 has autocorrelation function $\rho(0) = 1$, $\rho(i) = -\frac{1}{15}$ for $1 \leq i \leq 14$, as shown in Fig. 9.

Property VII—Autocorrelation Function: The autocorrelation function of a pseudo-random sequence of length $n = 2^m - 1$ is given by

$$\rho(0) = 1$$

$$\rho(i) = -1/n, \quad \text{for } 1 \leq i \leq 2^m - 2.$$

(For $a + a^{(i)} = a^{(j)}$ for some j by the shift-and-add property. Then D = number of 1's in $a^{(j)} = 2^{m-1}$, by Property IV, $A = n - D = 2^{m-1} - 1$, and the result follows from (11).)

It can be shown ([28, p. 48]) that this is the best possible autocorrelation function of any binary sequence of length $2^m - 1$, in the sense of minimizing $\max_{0<i<n} \rho(i)$.

E. Runs

Define a *run* to be a maximal string of consecutive identical symbols. For example, the first row of Fig. 6 contains runs of four 1's, three 0's, two 1's, two 0's, two runs of a single 1, and two runs of a single 0, for a total of 8 runs.

Property VIII—Runs: In any pseudo-random sequence, one-half of the runs have length 1, one-quarter have length 2, one-eighth have length 3, and so on, as long as these fractions give integral numbers of runs. In each case the number of runs of 0's is equal to the number of runs of 1's. (This follows easily from the window property—see [29, ch. 3].)

F. Random Sequences

Properties III, IV, VII, VIII justify the name pseudo-random sequences, for these are the properties that one would expect from a sequence obtained by tossing a fair coin $2^m - 1$ times. Such properties make pseudo-random sequences very useful in

a number of applications, such as range-finding [17a], [28, ch. 6], [52a], synchronizing [28, ch. 8], [65], modulation [28, ch. 5], scrambling [18], [39], [46], [57], etc.

Of course these sequences are not random, and one way this shows up is that the properties we have mentioned hold for *every* pseudo-random sequence, whereas in a coin-tossing experiment there would be some variation from sequence to sequence. For this reason these sequences are unsuitable for serious encryption ([21], [22]).

Property IX—A Test to Distinguish a Pseudo-Random Sequence from a Coin-Tossing Sequence (E. N. Gilbert [23]): Let $c_0, \cdots, c_{N-1}$ be N consecutive binary digits from a pseudo-random sequence of length $2^m - 1$, where $N < 2^m - 1$, where $N < 2^m - 1$, and form the matrix

$$M = \begin{bmatrix} c_0 & c_1 & \cdots & c_{N-b} \\ c_1 & c_2 & \cdots & c_{N-b+1} \\ \cdots & \cdots & \cdots & \cdots \\ c_{b-1} & c_b & \cdots & c_{N-1} \end{bmatrix}$$

where $m < b < \frac{1}{2}N$. Then the rank of M over $GF(2)$ is less than b. (From Property II, since there are only m linearly independent sequences in δ_m.) On the other hand, if $c_0, \cdots, c_{N-1}$ is a segment of a coin-tossing sequence, where each c_i is 0 or 1 with probability $\frac{1}{2}$, then the probability that rank $(M) < b$ can be shown to be at most 2^{2b-N-1}. This is very small if $b \ll \frac{1}{2}N$.

Thus the question, "is rank $(M) = b$?" is a test on a small number of digits from a pseudo-random sequence which shows a departure from true randomness. For example, if $m = 11$, $2^m - 1 = 2047$, $b = 15$, the test will fail if applied to any $N = 50$ consecutive digits of a pseudo-random sequence, whereas the probability that a coin-tossing sequence fails is at most 2^{-21}.

G. Hadamard Matrices

Recall that a *Hadamard matrix* is a real $n \times n$ matrix H_n of +1's and −1's which satisfies

$$H_n H_n^T = nI \tag{12}$$

where the T denotes transpose and I is an $n \times n$ unit matrix. (See for example Hall [35], Wallis *et al.* [71].)

Property X—Construction of Hadamard Matrices: Take the array whose rows are the sequences in δ_m, change 1's to −1's, and 0's to +1's, and add an initial column of +1's. The resulting $2^m \times 2^m$ array is a Hadamard matrix. (This follows from Property VII and equation (12).)

For example, Fig. 10 shows the 8×8 Hadamard matrix obtained in this way from the pseudo-random sequence 0010111.

Note that this Hadamard matrix can be constructed so that, except for the first row and column, it is a circulant matrix. For other Hadamard matrices with this property see [5], [67] and [28, Appendix 2].

H. Error-Correcting Codes

Definition: A binary linear *code* of *length* n, *dimension* k, and minimum *distance* d consists of 2^k binary vectors $u_1 \cdots u_n$, $u_i = 0$ or 1, called *codewords*, which: i) form a linear space (i.e. the modulo 2 sum of two codewords is a codeword), and ii) are such that any two codewords differ in at least d places. Such a code can correct $[\frac{1}{2}(d-1)]$ errors, where $[x]$ denotes the greatest integer not exceeding x. See for example [8], [44], or [52].

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & - & 1 & - & - & - \\ 1 & 1 & - & 1 & - & - & - & 1 \\ 1 & - & 1 & - & - & - & 1 & 1 \\ 1 & 1 & - & - & - & 1 & 1 & - \\ 1 & - & - & - & 1 & 1 & - & 1 \\ 1 & - & - & 1 & 1 & - & 1 & - \\ 1 & - & 1 & 1 & - & 1 & - & - \end{bmatrix}$$

(- STANDS FOR -1)

Fig. 10. An 8 × 8 Hadamard matrix.

For example $\mathcal{C}_1 = [000, 011, 101, 110]$ is a code of length 3, dimension 2, and minimum distance 2.

Property XI—Pseudo-Random Sequences form a Simplex Code: The sequences in δ_m form a linear code of length $2^m - 1$, dimension m, and minimum distance 2^{m-1}. All the nonzero codewords are cyclic shifts of any one of them. (From Properties, I, IV, V, and VI.)

For example the rows of Fig. 6 together with 0 form the code δ_4 of length 15, dimension 4, and minimum distance 8. Also $\mathcal{C}_1 = \delta_2$.

Let the weight of a vector $v = v_1 \cdots v_n$, denoted by $wt(v)$, be the number of nonzero v_i's, and let the Hamming distance between vectors $u = u_1 \cdots u_n$, $v = v_1 \cdots v_n$, denoted by dist (u, v), be the number of i's such that $u_i \neq v_i$. Clearly dist $(u, v) = wt(u - v)$. For example, dist $(1100, 1010) = wt(0110) = 2$. Exactly the same definitions apply to non-binary vectors. Condition ii) of the definition of a code requires that the codewords have Hamming distance at least d apart.

From Properties VII and IV any two codewords in δ_m have Hamming distance exactly 2^{m-1} apart, and for this reason δ_m is called a *simplex* code. (The codewords are at the vertices of a regular simplex.)

Let G_m be the $(2^m - 1) \times m$ matrix consisting of a list of the states of the shift register defined by $h(x)$, assuming that the initial state is $100 \cdots 0$. For example, G_4 is shown in Fig. 4. The columns of G_m are linearly independent. The set of all 2^m mod-2 linear combinations of these columns are exactly the sequences in δ_m. For this reason G_m is called a *generator matrix* for δ_m.

Definition: The *dual* code to δ_m, denoted by $\delta_m^\perp$, consists of all binary vectors u such that $uG_m = 0 \pmod 2$.

Then $\delta_m^\perp$ is a code of length $2^m - 1$ and dimension $2^m - 1 - m$. Since the rows of G_m are distinct, u is either zero or has at least three nonzero components. Hence $\delta_m^\perp$ has minimum distance 3. In fact $\delta_m^\perp$ is a Hamming single-error-correcting code (see [44, ch. 1]).

It is worth mentioning that coding theory provides the answers to the following questions, which sometimes arise in applications (see for example [9], [53], [66]):

i) Given a binary vector v of length $2^m - 1$, which pseudo-random sequence in δ_m is closest to it in Hamming distance? A fast way to find the answer uses a discrete version of the fast Fourier transform—see [33], [34], [44, ch. 14], [53], [73].

ii) How far away can a vector be from the closest pseudo-random sequence in δ_m? In other words, what is

$$f(m) = \max_{v} \min_{u \in \delta_m} \text{dist}\,(u, v)?$$

The vectors furthest away from δ_m are called *bent*—see [44, ch. 14], [17], [45], [56].

I. Representation of Pseudo-Random Sequences by Polynomials

The pseudo-random sequences in δ_m have a concise description by polynomials. We may represent any binary sequence $a = a_0 a_1 \cdots a_{n-1}$ of length n by the polynomial

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}. \tag{13}$$

For example 000100110101111 is represented by

$$a(x) = x^3 + x^6 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}. \tag{14}$$

A cyclic shift of a by one place to the right, $a_{n-1} a_0 a_1 \cdots a_{n-2}$, is represented by $a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1}$. If we agree that $x^n = 1$, then this is just $xa(x)$. For

$$\begin{aligned} xa(x) &= a_0 x + a_1 x^2 + \cdots + a_{n-2} x^{n-1} + a_{n-1} x^n \\ &= a_{n-1} + a_0 x + \cdots + a_{n-2} x^{n-1}. \end{aligned}$$

Multiplying by x corresponds to a cyclic shift to the right.

A primitive polynomial $h(x)$ of degree m always divides $x^n + 1$, where $n = 2^m - 1$ and the division is carried out modulo 2 ([44, ch. 4]). Let

$$\tilde{h}(x) = \sum_{k=0}^{m} h_k x^{m-k} = x^m h\left(\frac{1}{x}\right). \tag{15}$$

This is the *reciprocal polynomial* of $h(x)$, obtained by reversing the coefficients. Define

$$g(x) = \frac{x^n + 1}{\tilde{h}(x)}. \tag{16}$$

E.g. if $h(x) = x^4 + x + 1$, $\tilde{h}(x) = x^4 + x^3 + 1$, and

$$g(x) = \frac{x^{15} + 1}{x^4 + x^3 + 1} = 1 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{10} + x^{11}. \tag{17}$$

Notice that (14) is x^3 times (17). This is a special case of

Property XII—Polynomial Representation: The pseudo-random sequences in δ_m consist of the polynomials $x^i b(x)$, $i = 0, \cdots, 2^m - 2$, where $b(x)$ is any polynomial in δ_m (from Properties I or XI). Alternatively, they are the polynomials $t(x)g(x)$ where $t(x)$ is any polynomial of degree less than m.

(For let $b(x) = t(x)g(x) = \sum_{j=0}^{n-1} b_j x^j$. Then $b(x)\tilde{h}(x) = t(x)(x^m + 1)$. Equating coefficients of x^{m+i} in this identity gives

$$\sum_{k=0}^{m} b_{i+k} h_k = 0, \qquad i = 0, \cdots, n - m - 1.$$

But this is the recurrence of Property II, so $b(x) \in \delta_m$. Since $g(x), xg(x), \cdots, x^{m-1} g(x)$ represent m linearly independent sequences in δ_m, everything in δ_m can be represented by $t(x)g(x)$ where $\deg t(x) < m$.)

Hence $g(x)$ is distinguished by being the polynomial of lowest degree in δ_m, and is called the *generator polynomial* of δ_m.

J. Finite Fields

A *field* is a set of elements in which it is possible to add, subtract, multiply, and divide. For any α, β, γ in the field we must have

$$\alpha + \beta = \beta + \alpha, \qquad \alpha\beta = \beta\alpha$$

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma, \qquad \alpha(\beta\gamma) = (\alpha\beta)\gamma$$

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$$

and, furthermore, elements 0, 1, $-\alpha$, and (for $\alpha \neq 0$) α^{-1} must exist such that

$$0 + \alpha = \alpha, \qquad (-\alpha) + \alpha = 0, \qquad 0\alpha = 0$$

$$1\alpha = \alpha, \qquad (\alpha^{-1})\alpha = 1.$$

A *finite* field contains a finite number of elements. A field with q elements is called a *Galois field* and is denoted by $GF(q)$.

The simplest fields are the following: Let p be a prime number. Then the integers modulo p form the field $GF(p)$. The elements of $GF(p)$ are $\{0, 1, 2, \cdots, p - 1\}$, and $+, -, \times, \div$ are carried out mod p. For example, $GF(2)$ is the binary field $\{0, 1\}$. $GF(3)$ is the ternary field $\{0, 1, 2\}$, with $1 + 2 = 3 = 0 \pmod 3$, $2 \cdot 2 = 4 = 1 \pmod 3$, $1 - 2 = -1 = 2 \pmod 3$, etc.

A field with p^m elements, when p is a prime and m is any positive integer, can be constructed as follows. The elements of the field are all polynomials in x of degree $\leqslant m - 1$ with coefficients from $GF(p)$. Addition is done in the ordinary way, modulo p.

A polynomial with coefficients from $GF(p)$ which is not the product of two polynomials of lower degree is called *irreducible*. A primitive polynomial is automatically irreducible. Choose a fixed irreducible polynomial $h(x)$ of degree m.

Then the product of two field elements is obtained by multiplying them in the usual way (modulo p), and taking the remainder when divided by $h(x)$. The field obtained in this way contains p^m elements and is denoted by $GF(p^m)$.

As in illustration we take $p = 2$, $m = 4$, $h(x) = x^4 + x + 1$ and construct $GF(2^m)$. The 16 elements are

$$0, 1, x, x + 1, x^2 + 1, \cdots, \qquad x^4 + x^3 + x^2 + x + 1.$$

Addition is like this

$$(x^2 + 1) + (x + 1) = x^2 + x$$

and multiplication like this: The ordinary product of $x^3 + 1$ and $x^3 + x + 1$ is $x^6 + x^4 + x + 1$. But

$$x^6 + x^4 + x + 1 = (x^2 + 1)h(x) + x^3 + x^2$$

so in the field

$$(x^3 + 1)(x^3 + x + 1) = x^3 + x^2.$$

It is easy to check that this set has all the properties of a field; the inverses $a(x)^{-1}$ exist because $h(x)$ is irreducible (see [44, chs. 3, 4], [4], [6], [8] or [15] for details).

Just as complex numbers can be written either in rectangular coordinates, as $z = x + iy$, or in polar coordinates, as $z = re^{i\theta}$, so elements of a finite field have two representations. The first is the polynomial form given above, and the second is as a power of a certain fixed field element called a *primitive* element, denoted by ξ. (If $h(x)$ is a primitive polynomial we can take ξ to be a zero of $h(x)$.)

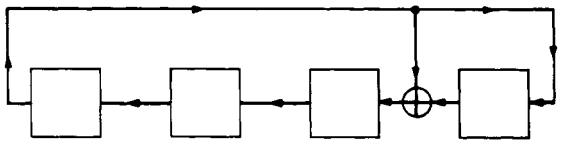
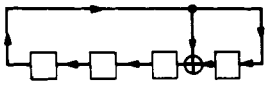


Fig. 11. A shift register generating the elements of $GF(2^4)$.



AS A POLYNOMIAL				AS A POWER OF ξ
0	0	0	1	1
0	0	1	0	ξ
0	1	0	0	ξ^2
1	0	0	0	ξ^3
0	0	1	1	ξ^4
0	1	1	0	ξ^5
1	1	0	0	ξ^6
1	0	1	1	ξ^7
0	1	0	1	ξ^8
1	0	1	0	ξ^9
0	1	1	1	ξ^{10}
1	1	1	0	ξ^{11}
1	1	1	1	ξ^{12}
1	1	0	1	ξ^{13}
1	0	0	1	ξ^{14}
0	0	0	1	$\xi^{15} = 1$
	•	•	•	• • •

Fig. 12. The elements of the field $GF(2^4)$.

Assuming that $h(x)$ is a primitive polynomial, the correspondence between the two forms can be obtained from a shift register. This shift register is the reverse of that in Fig. 2. E.g. if $h(x) = x^4 + x + 1$, the shift register is shown in Fig. 11. The states of this shift register provide a list of the elements of $GF(2^4)$, both as successive powers of ξ and as polynomials in x of degree at most three (see Fig. 12, where only the coefficients of the polynomials are given).

A finite field of order p^m exists for all primes p and positive integers m. Furthermore these are the only finite fields (see [44, ch. 4]).

If $\beta \in GF(p^m)$, the sum

$$T_m(\beta) = \beta + \beta^p + \beta^{p^2} + \cdots + \beta^{p^{m-1}}$$

is called the *trace* of β. The trace has the following properties:

i) $T_m(\beta) \in GF(p)$.
ii) $T_m(\beta + \gamma) = T_m(\beta) + T_m(\gamma)$, $\beta, \gamma \in GF(p^m)$.
iii) $T_m(\beta)$ takes on each value in $GF(p)$ equally often, i.e., p^{m-1} times, as β ranges over $GF(p^m)$.
iv) $T_m(\beta^p) = T_m(\beta)^p = T_m(\beta)$.
v) $T_m(1) \equiv m \pmod p$.

K. Pseudo-Random Sequences Form a Field

As before, let δ_m be the set of pseudo-random sequences of length $n = 2^m - 1$, obtained from a primitive polynomial $h(x)$ of degree m. It is clear how to add two elements of δ_m. Multiplication is carried out using the polynomial representation given in Section II-I. That is, two polynomials are multiplied in the usual way (mod 2), and then x^n is replaced by 1, x^{n+1} by x, and so on. The result is another element of δ_m.

Property XIII – δ_m is a Field: With this definition of addition and multiplication, δ_m is isomorphic to the field $GF(2^m)$.

Let ξ be a primitive element of $GF(2^m)$ which is a zero of $h(x)$, as in the previous section. Then ξ^{-1} is a zero of $\tilde{h}(x)$, and $g(\xi^{-1}) \neq 0$. From Property XII, $b(\xi^{-1}) \neq 0$ for all nonzero $b(x) \in \delta_m$.

The isomorphism between δ_m and $GF(2^m)$ is given by

$$b(x) \in \delta_m \xrightarrow{\varphi} b(\xi^{-1}) \in GF(2^m)$$

and

$$\gamma \in GF(2^m) \xrightarrow{\psi} (b_0 b_1 \cdots b_{n-1}) \in \delta_m$$

where $b_i = T_m(\gamma \xi^i)$. For the proof of all this see [44, ch. 8].

The element $E(x) = \sum_{i=0}^{n-1} E_i x^i$ of δ_m which maps onto $1 \in GF(2^m)$ must satisfy $E(x)^2 = E(x)$. This element is called the *idempotent* of δ_m and has the property that $E_i = E_{2i}$ (subscripts modulo n) [27]. It is found as follows: Since n is odd, $x^n + 1$ has distinct factors over $GF(2)$. Therefore $g(x)$ and $\tilde{h}(x)$ are relatively prime and so there exist polynomials $u(x)$, $v(x)$ such that

$$u(x)g(x) + v(x)\tilde{h}(x) \equiv 1 \pmod 2 \qquad (18)$$

and $\deg u(x) < m$ ([47], [70]). Setting $x^n = 1$ gives

$$g(x)\tilde{h}(x) = 0$$

and, multiplying (18) by $u(x)g(x)$,

$$(u(x)g(x))^2 = u(x)g(x).$$

Therefore $E(x) = u(x)g(x)$ is the idempotent of δ_m. Then

$$E(x) \xrightarrow{\varphi} 1$$

$$xE(x) \xrightarrow{\varphi} \xi^1.$$

For any $b(x) \in \delta_m$ there is a $c(x) \in \delta_m$ such that $b(x)c(x) = E(x)$. In fact if $b(x) = x^i E(x)$ (for every nonzero sequence in δ_m is a cyclic shift of $E(x)$) then $c(x) = x^{n-i}E(x)$.

Example: With $h(x) = x^4 + x + 1$, $\tilde{h}(x) = x^4 + x^3 + 1$, and $g(x)$ given by (17), we find

$$x^3 g(x) + (1 + x^4 + x^6 + x^8 + x^{10})\tilde{h}(x) = 1$$

so that $E(x) = x^3 g(x)$, given by (14), is the idempotent.

III. Pseudo-Random Arrays

A. Two-Dimensional Arrays with Flat Autocorrelation Functions

These can be constructed by folding pseudo-random sequences. Take a number of the form $n = 2^{k_1 k_2} - 1$ such that $n_1 = 2^{k_1} - 1$ and[1] $n_2 = n/n_1$ are relatively prime and greater than 1. Then $n = n_1 n_2$. Examples are

$n = 15 = 2^4 - 1$ with $k_1 = k_2 = 2$, $n_1 = 3$, $n_2 = 5$

$n = 63 = 2^6 - 1$ with $k_1 = 3$, $k_2 = 2$, $n_1 = 7$, $n_2 = 9$

$n = 511 = 2^9 - 1$ with $k_1 = 3$, $k_2 = 3$, $n_1 = 7$, $n_2 = 73$.

The starting point is a pseudo-random sequence $\boldsymbol{a} =$

[1] $2^{k_1} - 1$ always divides $2^{k_1 k_2} - 1$.

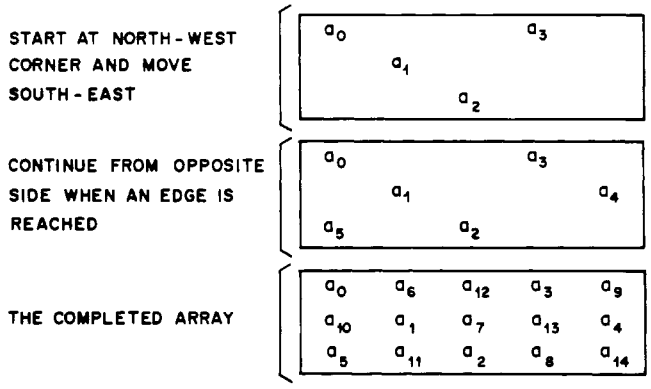


Fig. 13. Constructing a pseudo-random array.

A 3 BY 5 PSEUDO-RANDOM ARRAY

```
1111
 11
1  1
```

A 7 BY 9 PSEUDO-RANDOM ARRAY

```
  1  1
 111111
1 1111 1
1  11  1
111  111
 1 11 1
11    11
```

A 15 BY 17 PSEUDO-RANDOM ARRAY

```
   1 1 1 1    11
 11 1 1 11  1  1
11   1 1   111111
1 1 11 11 1 11111
  1       1  1111
1111     1111 11
 11 1   1 11
1   11 11   1
11 1     1 111  1
1  11   11  1 11
111  1 1  111
 1 111 111 1 1  1
 1  1   1  1 1111
 11111 11111  11
1 111   111 11  1
```

A 31 BY 33 PSEUDO-RANDOM ARRAY

```
 1 1 1   11 1    1  1    1 11   1
     11   1   1 1111 1   1   11
11 1111 1 11 11  1111  11 11 1 11
    1 1 1  111 111111 111  1 1 1
 1 1 1 11  111 11    11 111  11 1
11 11 1     11 1 1  1 1 11      1
1   1  111  1111 1  1 1111  111
11 11   111 1  11111111  1 111
1   111  11  1 1       1 1  11  11
1   1 1 11 1111   11   1111 11 1
     11  1 111111    111111 1  11
1   1 11  1 1 1111111111 1 1  11
11 11111 1    111 11 111    1 111
11 111   1 1  1 11  11 1  1 1   1
      1 111  1  1 11 1  1  111 1
     1111 1 1 1  1  1  1 1 1 1111
 1 1  1   11 11111  11111 11   1
1   1     111 1 1    1 1 111
       11111 1 111  111 1 11111
11 11  1   111    11    111   1
 1 1 111 1111  1  11  1 1111 111
11 111 11 1  111      111  1 11 1
11 11 1111111   1    1   1111111
 1 1    11 1  11 1111 11  1 11
1   11111  1    11  11    1  1111
 1 1  1111    1        1    1111
 1 1   1  1  11 1 11 1 11  1  1
 1 1 11 1   11  111111  11   1 11
     1  1 111 11  11  11 111 1  1
1   11  1       11 11 11      1  1
1   11 1 111 1   1111   1 111 1 1
```

Fig. 14. Examples of pseudo-random arrays.

$a_0a_1 \cdots a_{n-1}$ in $\delta_{k_1k_2}$, obtained from a primitive polynomial $h(x)$ of degree $m = k_1k_2$. We use a to fill up an $n_1 \times n_2$ array, by writing a down the main diagonal and continuing from the opposite side whenever an edge is reached. Fig. 13 shows the construction when $n = 15$, $n_1 = 3$, $n_2 = 5$. Thus the pseudo-random sequence

$$000100110101111 \tag{19}$$

produces the array

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}. \tag{20}$$

This is the top array in Fig. 14.

An $n_1 \times n_2$ array formed in this way will be called a *pseudo-random array*. There are n different arrays, one from each pseudo-random sequence in $\delta_{k_1k_2}$. Fig. 14 shows examples of 3×5, 7×9, 15×17, and 31×33 pseudo-random arrays, the first three constructed from pseudo-random sequences in Fig. 7 and the fourth from the sequence defined by $h(x) = x^{10} + x^3 + 1$ (from Fig. 5). In Fig. 14 zeros have been replaced by blanks; in the first two arrays the left-hand column is completely blank.

The pseudo-random sequences in $\delta_{k_1k_2}$ at least look random to the eye, whereas the corresponding arrays have a conspicuous nonrandom feature, being symmetric about a column of zeros. Nevertheless we call them pseudo-random arrays because they share Properties III*, IV* and VII* below with an array formed by tossing a coin.

To state these properties some further notation is required. If the pseudo-random array is denoted by

$$b = \begin{bmatrix} b_{00} & b_{01} & \cdots & b_{0,n_2-1} \\ b_{10} & b_{11} & \cdots & b_{1,n_2-1} \\ \cdots & & \cdots & \cdots \\ b_{n_1-1,0} & & \cdots & b_{n_1-1,n_2-1} \end{bmatrix} \tag{21}$$

then

$$\begin{aligned} a_0 &= b_{00} \\ a_1 &= b_{11} \\ a_2 &= b_{22} \\ &\cdots \end{aligned}$$

and

$$a_i = b_{i_1 i_2} \tag{22}$$

where

$$\begin{aligned} i &\equiv i_1 \pmod{n_1}, \quad 0 \leqslant i_1 < n_1 \\ i &\equiv i_2 \pmod{n_2}, \quad 0 \leqslant i_2 < n_2. \end{aligned} \tag{23}$$

Conversely, given i_1 and i_2 with $0 \leqslant i_1 < n_1$ and $0 \leqslant i_2 < n_2$, there is a unique value of i in the range $0 \leqslant i < n = n_1 n_2$ such that (23) holds, by the Chinese Remainder Theorem (since n_1 and n_2 are relatively prime)—see [47, p. 33] or [70, pp. 189–191].

These arrays are best described by polynomials. The array (21) is represented by

$$b(x,y) = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} b_{ij} x^i y^j. \tag{24}$$

E.g. (20) is

$$b(x,y) = (y + y^2 + y^3 + y^4) + x(y^2 + y^3) + x^2(y + y^4). \tag{25}$$

If we agree that $x^{n_1} = 1$ and $y^{n_2} = 1$, then multiplying $b(x,y)$ by x corresponds to a cyclic shift of the array downwards, and multiplying by y corresponds to a cyclic shift to the right.

B. Properties of Pseudo-Random Arrays

With n, n_1, n_2, k_1, k_2 as defined above, let $h(z)$ be a fixed primitive polynomial of degree $m = k_1 k_2$. Each of the pseudo-random sequences in $\mathcal{S}_m$ folds into a distinct $n_1 \times n_2$ pseudo-random array. Let $\mathcal{A}_m$ be the set of 2^m arrays so formed, together with the zero array. We briefly state the properties of these arrays.

Property XII—Polynomial Representation:* Suppose the pseudo-random sequence a folds up to produce the array b. The polynomial $b(x,y)$ describing b is obtained from $a(z) = \sum_{i=0}^{n-1} a_i z^i$ by replacing z by xy:

$$b(x,y) = a(xy). \tag{26}$$

(For this replaces each term $a_i z^i$ in $a(z)$ by $a_i x^{i_1} y^{i_2}$ where $i \equiv i_1 \pmod{n_1}$, $0 \leqslant i_1 < n_1$ and $i \equiv i_2 \pmod{n_2}$, $0 \leqslant i_2 < n_2$. Thus a_i goes into the square (i_1, i_2) of the array: $b_{i_1 i_2} = a_i$, in agreement with (22).)

E.g. (19) is described by

$$a(z) = z^3 + z^6 + z^7 + z^9 + z^{11} + z^{12} + z^{13} + z^{14}$$

and replacing z by xy with $x^3 = y^5 = 1$ we obtain

$$b(x,y) = a(xy) = y^3 + y + xy^2 + y^4 + x^2 y + y^2 + xy^3 + x^2 y^4$$

in agreement with (25).

Property I—The Shift Property:* If b (equation (21)) is a pseudo-random array in $\mathcal{A}_m$, so is any cyclic shift of b downwards or to the right,

$$\begin{bmatrix} b_{i0} & \cdots & b_{i,n_2-1} \\ \cdots & \cdots & \cdots \\ b_{i-1,0} & \cdots & b_{i-1,n_2-1} \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} b_{0j} & \cdots & b_{0,j-1} \\ \cdots & \cdots & \cdots \\ b_{n_1-1,j} & \cdots & b_{n_1-1,j-1} \end{bmatrix} \tag{27}$$

or any combination of these shifts.

(Since n_1 and n_2 are relatively prime there are integers μ and ν such that

$$\mu n_1 + \nu n_2 = 1. \tag{28}$$

E.g. if $n_1 = 3, n_2 = 5$, $2 \cdot 3 - 5 = 1$, and $\mu = 2, \nu = -1$. Then

$$z^{\nu n_2} = x^{\nu n_2} y^{\nu n_2} = x^{\nu n_2} = x^{\nu n_2} x^{\mu n_1} = x$$

and similarly $z^{\mu n_1} = y$. Therefore the arrays (27) are $x^i b(x,y) = z^{i\nu n_2} a(z)$ and $y^j b(x,y) = z^{j\mu n_1} a(z)$, both in $\mathcal{A}_m$.)

The pseudo-random arrays in $\mathcal{A}_m$ are represented by the polynomials $x^{i_1} y^{i_2} b(x,y)$, $0 \leqslant i_1 < n_1$, $0 \leqslant i_2 < n_2$, where $b(x,y)$ is any array in $\mathcal{A}_m$. Alternatively they are the polynomials $t(x,y)\gamma(x,y)$, where $\deg_x t(x,y) < n_1$, $\deg_y t(x,y) < n_2$, $\gamma(x,y) = g(xy)$, and $g(z)$ is the generator polynomial of $\mathcal{S}_m$. E.g. in $\mathcal{A}_4$ from (17) we obtain

$$\gamma(x,y) = (1 + y + y^3 + y^4) + x(1 + y^4) + x^2(y + y^3)$$

corresponding to

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Property II—Recurrences:* Equation (9) implies that a pseudo-random array in $\mathcal{A}_m$ satisfies a recurrence along the diagonals. E.g. from (4), (20) satisfies

$$b_{i+4,i+4} = b_{i+1,i+1} + b_{i,i}.$$

It is also possible to find a *pair* of recurrences which generate the array, one for moving vertically and one horizontally. We illustrate this by two examples, but omit the general proof. For (20) the recurrences are

$$\begin{aligned} b_{i+2,j} &= b_{i+1,j} + b_{i,j} \quad \text{(vertically)} \\ b_{i,j+2} &= b_{i+2,j+1} + b_{i,j} \quad \text{(horizontally).} \end{aligned} \tag{29}$$

For the 15×17 array in Fig. 14 they are

$$\begin{aligned} b_{i+4,j} &= b_{i+1,j} + b_{i,j} \quad \text{(vertically)} \\ b_{i,j+2} &= b_{i+1,j+1} + b_{i,j+1} + b_{i,j} \quad \text{(horizontally).} \end{aligned} \tag{30}$$

From these recurrences the $k_1 \times k_2$ subarray in the North-West corner determines the entire array.

Property III—The Window Property:* If a $k_1 \times k_2$ window is slid over a pseudo-random array in $\mathcal{A}_m$, each of the $2^{k_1 k_2} - 1$ nonzero binary $k_1 \times k_2$ arrays is seen exactly once—see Fig. 15 for the case $n = 15$, $k_1 = k_2 = 2$. (The proof is given in the Appendix.)

Property IV—Half 0's and Half 1's:* Any array in $\mathcal{A}_m$ contains 2^{m-1} 1's and $2^{m-1} - 1$ 0's.

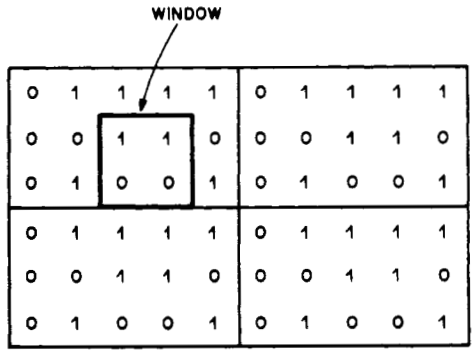


Fig. 15. The window property: Every nonzero 2 × 2 array is seen once.

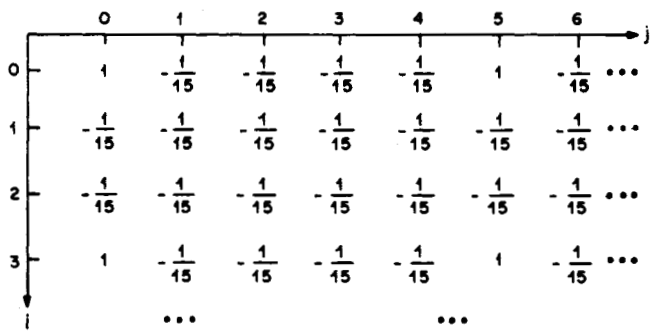


Fig. 16. Autocorrelation function $\rho(i,j)$ of a pseudo-random array.

Property V—The Addition Property:* The sum of two arrays in $\mathfrak{A}_m$ is again in $\mathfrak{A}_m$.

Property VI—The Shift-and-Add Property:* The sum of $b(x,y) \in \mathfrak{A}_m$ and any shift $x^i y^j b(x,y)$ is another array in $\mathfrak{A}_m$. (These follow from Properties IV, V, VI.)

C. Autocorrelation Function

Let b (equation (21)) be any $n_1 \times n_2$ array of area $n = n_1 \times n_2$. The *(two-dimensional) autocorrelation function* of b, $\rho(i,j)$, is defined as follows. If A is the number of positions in which b and b shifted i places down and j to the right agree, and D is the number in which they disagree, then

$$\rho(i,j) = \frac{A-D}{n}, \quad i,j = 0, \quad \pm 1, \pm 2, \cdots. \tag{31}$$

Again $A + D = n$. This is a doubly periodic function with $\rho(i,j) = \rho(i+n_1, j) = \rho(i, j+n_2)$, $\rho(0,0) = \rho(n_1, 0) = \cdots = 1$. For example, Fig. 16 shows the autocorrelation function of (20).

Property VII—Autocorrelation Function:* The two-dimensional autocorrelation function of a pseudo-random array in $\mathfrak{A}_m$ is given by

$$\rho(0,0) = 1$$

$$\rho(i,j) = -\frac{1}{n}, \quad 0 \leqslant i < n_1, \quad 0 \leqslant j < n_2, \quad (i,j) \neq (0,0). \tag{32}$$

(From Properties VI*, IV*). Again this is best possible.

D. Other Constructions of Pseudo-Random Arrays

i) A pseudo-random sequence of length $n = 2^m - 1$ can be folded into an $n_1 \times n_2$ array as shown in Fig. 13 whenever $n = n_1 n_2$ and n_1, n_2 are relatively prime. The resulting array still has Properties XII*, I*, IV*, V*, and VI*.

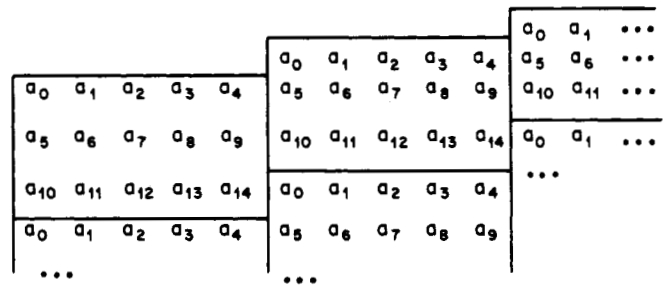


Fig. 17. Another construction of a pseudo-random array.

deg	$q = 3$	$q = 4$	$q = 8$
1	$x+1$	$x+\omega$	$x+\alpha$
2	x^2+x+2	$x^2+x+\omega$	$x^2+\alpha x+\alpha$
3	x^3+2x+1	$x^3+x^2+x+\omega$	$x^3+x+\alpha$
4	x^4+x+2	$x^4+x^2+\omega x+\omega^2$	$x^4+x+\alpha^3$
5	x^5+2x+1	$x^5+x+\omega$	$x^5+x^2+x+\alpha^3$
6	x^6+x+2	$x^6+x^2+x+\omega$	$x^6+x+\alpha$
7	$x^7+x^6+x^4+1$	$x^7+x^2+\omega x+\omega^2$	$x^7+x^2+\alpha x+\alpha^3$
8	x^8+x^5+2	$x^8+x^3+x+\omega$	
9	$x^9+x^7+x^5+1$	$x^9+x^2+x+\omega$	
10	$x^{10}+x^9+x^7+2$	$x^{10}+x^3+\omega(x^2+x+1)$	

Fig. 18. Primitive polynomials over $GF(q)$.

ii) Another way of making pseudo-random sequences into arrays has been suggested by Spann [63]. This applies when the whole plane is to be filled with copies of the array. Let $a_0 \cdots a_{n-1}$ be a pseudo-random sequence of length $n = 2^m - 1 = n_1 n_2$, where n_1 and n_2 may have a common factor. The infinite array $\{b_{ij}: i,j = 0, \pm 1, \cdots\}$ is formed by setting $b_{ij} = a_k$, where $k \equiv in_1 + j \pmod{n_2}$ and $0 \leqslant k \leqslant n-1$. Fig. 17 illustrates the construction in the case $n = 15$, $n_1 = 3$, $n_2 = 5$. The autocorrelation function of the $n_1 \times n_2$ rectangle $\{b_{ij}: 0 \leqslant i < n_1, 0 \leqslant j < n_2\}$ is not in general given by (32). However if we define the periodic autocorrelation function of the infinite array to be

$$\overline{\rho}(i,j) = \frac{1}{n} \sum_{r=0}^{n_1-1} \sum_{s=0}^{n_2-1} (-1)^{b_{rs}+b_{r+i,s+j}} \tag{33}$$

then $\overline{\rho}(i,j)$ *is* given by (32).

IV. Nonbinary Pseudo-Random Sequences and Displays

A. Arrays with Entries from an Alphabet of q Symbols

The same constructions can be used to obtain pseudo-random sequences and arrays with entries which, instead of being 0's and 1's, are taken from an alphabet of q symbols, for any q which is a prime or a power of a prime.

Let q be any prime power and let $GF(q)$ be the Galois field with q elements (see Section II-J). We need a polynomial $h(x)$ of degree m with coefficients from $GF(q)$ which i) is not the product of two such polynomials of lower degree, and ii) has as a zero a primitive element of $GF(q^m)$, say ξ. We call such a polynomial *primitive over* $GF(q)$. The primitive polynomials used in Section II are primitive over $GF(2)$. Fig. 18 gives a small table of primitive polynomials, using $GF(4) = \{0, 1, \omega, \omega^2\}$, with $\omega^2 + \omega + 1 = 0$, $\omega^3 = 1$, and

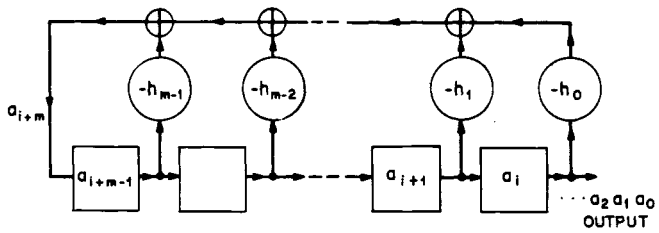


Fig. 19. Shift register specified by $h(x)$.

length 8 over GF(3)

01220211

length 26 over GF(3)

00101211201110020212210222

length 80 over GF(3)

00010021011120022010221101012122120122220002001202
22100110201122020212112102111 1

length 242 over GF(3)

00001000120011101C021202211202011211012021112200 10
10121211212012111120001100102012211102002210202221
20021102202201201111100002000210022202001210112210
10221220210122211002020212122121021222210002200201
02112220100112010111210012201101102102222?

length 15 over GF(4)

011310221203323

length 63 over GF(4)

00110312223221020213100220123331332030321200330231
1121130101323

length 255 over GF(4)

00010122022311110013113123232223010320312020332213
30133112131030012101321003332011031000303110112333
30032332312121112030210231010221132203223313230200
31303213002221033023000202330331222200212212313133
31020130123030113321102112232120100232021320011130
22012

Fig. 20. Pseudo-random sequences over $GF(3)$ and $GF(4)$.

$GF(8) = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^6\}$ with $\alpha^3 + \alpha + 1 = 0$, $\alpha^7 = 1$. For more extensive tables see [1], [7], [15], [32], [46], [52], [64].

Suppose

$$h(x) = x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + h_0 \qquad (34)$$

with $h_i \in GF(q)$, $h_0 \neq 0$. The shift register specified by $h(x)$ is shown in Fig. 19. In this figure the boxes contain elements of $GF(q)$, say $a_{i+m-1}, \cdots, a_i$. The feedback path then forms

$$a_{i+m} = -h_{m-1}a_{i+m-1} - h_{m-2}a_{i+m-2} - \cdots - h_1 a_{i+1} - h_0 a_i. \qquad (35)$$

0213233311333231 2
0013321033012331 0
0300223133132200 3
0121203200230212 1
0332030111103023 3
0321311122111312 3
0021132011023112 0
0100331211213300 1
0232301300310323 2
0113010222201031 1
0132122233222123 1
0032213022031223 0
0200112322321100 2
0313102100120131 3
0221020333302012 2

Fig. 21. A 15 X 17 pseudo-random array with entries from the field of 4 elements.

Equation (35) is the recurrence describing the output sequence. This is an infinite sequence of period $q^m - 1$ (if the starting state is not zero), and each nonzero state appears once in a period. A segment of the output sequence of length $q^m - 1$ is called a *pseudo-random sequence over* $GF(q)$. Let $\delta_m(q)$ be the set of such sequences, together with **0**. (See [3], [11], [14], [24], [25], [60], [76].)

For example, if $q = 4$, $m = 2$, and $h(x) = x^2 + x + \omega$ we obtain the pseudo-random sequence

$$0\ 1\ 1\ \omega^2\ 1\ 0\ \omega\ \omega\ 1\ \omega\ 0\ \omega^2\ \omega^2\ \omega\ \omega^2 \qquad (36)$$

of length 15. Then $\delta_2(4)$ consists of **0** and the 15 cyclic shifts of (36). Fig. 20 shows some pseudo-random sequences over $GF(3)$ and $GF(4)$, where in $GF(4)$ ω is replaced by 2 and ω^2 by 3.

Pseudo-random arrays can be obtained as in Section III. For example Fig. 21 shows a 15 X 17 array over $GF(4)$ obtained by folding the length 255 sequence in Fig. 20.

B. Some Properties.

Properties I, II, III, V, VI hold with obvious changes, while Property IV is replaced by:

*Property IV**:* In any pseudo-random sequence in $\delta_m(q)$ 0 occurs $q^{m-1} - 1$ times and every nonzero element of $GF(q)$ occurs q^{m-1} times.

Instead of Property VII we have the following.

Property VIIa: A pseudo-random sequence in $\delta_m(q)$ has the form

$$a = b, \gamma b, \gamma^2 b, \cdots, \gamma^{q-2} b, \qquad (37)$$

where b is a sequence of length $(q^m - 1)/(q - 1)$ and γ is a primitive element of $GF(q)$. (This is because the states of the shift register can be made to correspond to a logarithm table of $GF(q)$. The details are omitted).

For example in (36), $b = 011\omega^2 1$ and $\gamma = \omega$. For some applications b is a more useful sequence than a.

Property VIIb: Let $a = (a_0 \cdots a_{n-1})$ be a pseudo-random sequence in $\delta_m(q)$, and let $b = (a_s a_{s+1} \cdots a_{s-1}) = (b_0 \cdots b_{n-1})$ be a shift of a by s places. i) If s is not a multiple of $q - 1$, then among the $q^m - 1$ pairs (a_i, b_i), (0, 0) occurs $q^{m-2} - 1$ times and every other pair of elements of $GF(q)$ occurs q^{m-2} times; ii) If $s = j(q - 1)$, then (0, 0) occurs $q^{m-1} - 1$ times and the pairs $(\alpha, \gamma^j\alpha)$, for all nonzero α in $GF(q)$, occur q^{m-1} times.

In particular, if $s = 0$ (no shift) each (α, α), $\alpha \neq 0$, occurs q^{m-1} times. For example, if (36) is shifted once, thus

$$0\ 1\ 1\ \omega^2\ 1\ 0\ \omega\ \omega\ 1\ \omega\ 0\ \omega^2\ \omega^2\ \omega\ \omega^2$$
$$1\ 1\ \omega^2\ 1\ 0\ \omega\ \omega\ 1\ \omega\ 0\ \omega^2\ \omega^2\ \omega\ \omega^2\ 0$$

then $(0, 0)$ does not occur and every other pair $(0, 1)$, $(0, \omega)$, $\cdots$, (ω^2, ω^2) occurs once.

There are many ways of obtaining a real- or complex-valued sequence from a sequence in $\delta_m(q)$. We shall just consider the case q = prime and the complex-valued sequence $\hat{a}$ obtained from $a \in \delta_m(q)$ by replacing $r \in GF(q)$ by $e^{2\pi ir/q}$.

Property VIIc—Autocorrelation function: The autocorrelation function of $\hat{a}$ is given by

$$\rho(0) = 1, \qquad \rho(i) = -\frac{1}{q^m - 1}, \qquad 1 \leq i \leq q^m - 2.$$

(Immediate from Property VIIb.) For other autocorrelation functions, all of which can be calculated from Property VIIb, see [3], [11], [14], [25], [76].

V. Transmission Functions

The following question has arisen in certain optical applications (Knowlton [43]). For a given value q, say $q = 2, 3, 4, \cdots$, find a set of q $n_1 \times n_2$ arrays of 0's and 1's whose transmission function $\tau(r, s)$ is zero at the origin and approximately constant elsewhere. The *transmission function* τ is defined as follows. If the q arrays are (a_{ij}), (b_{ij}), (c_{ij}), $\cdots$ then

$$\tau(r, s) = \frac{1}{n_1 n_2} \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} \cdot (1 - a_{ij})(1 - b_{i+r,j+s})(1 - c_{i+2r,j+2s}) \cdots \quad (38)$$

where the first subscript is taken modulo n_1, and the second modulo n_2, and the sum is evaluated as a real number. This is doubly periodic: $\tau(r, s) = \tau(r + n_1, s) = \tau(r, s + n_2)$.

Arrays with these properties can be obtained from pseudo-random sequences, as will be shown.

Case $q = 2$: Let $(a_{ij}) \in a_m$ be an $n_1 \times n_2$ pseudo-random array as constructed in Section III, where $n = n_1 n_2 = 2^m - 1$, and let (b_{ij}) be its complement: $b_{ij} = 1 - a_{ij}$. Then $\tau(0, 0) = 0$ and

$$\tau(r, s) = \frac{1}{n} (\text{number of times } a_{ij} = 0 \text{ and } a_{i+r,j+s} = 1)$$
$$= \frac{2^{m-2}}{2^m - 1} (\text{from Properties I, IV, V}) \quad (39)$$

for all $0 \leq r \leq n_1 - 1$, $0 \leq s \leq n_2 - 1$, $(r, s) \neq (0, 0)$.

Case q = Prime Power: For ease of notation we take $q = 4$; the general case is similar. Let (A_{ij}) be an $n_1 \times n_2$ pseudo-random array over $GF(4)$ as constructed in Section IV, where $n = n_1 n_2 = 4^m - 1$, $m \geq 4$. The A_{ij}'s are 0, 1, ω or ω^2. The desired binary arrays are given by

$$a_{ij} = 1 \text{ if and only if } A_{ij} = 0$$
$$b_{ij} = 1 \text{ if and only if } A_{ij} = 1$$
$$c_{ij} = 1 \text{ if and only if } A_{ij} = \omega$$
$$d_{ij} = 1 \text{ if and only if } A_{ij} = \omega^2. \quad (40)$$

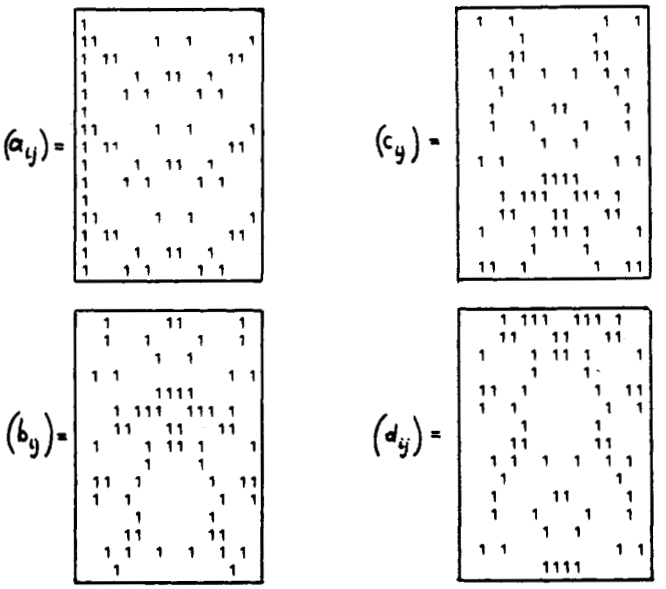


Fig. 22. Four 15 × 17 arrays obtained from Fig. 21.

Fig. 22 shows the four 15×17 arrays obtained in this way from Fig. 21.

The transmission function is given by

$$\tau(r, s) = \frac{1}{n_1 n_2} (\text{number of times } A_{ij} \neq 0, A_{i+r,j+s} \neq 1 \cdot A_{i+2r,j+2s} \neq \omega \text{ and } A_{i+3r,j+3s} \neq \omega^2). \quad (41)$$

Define t by $0 \leq t < n_1 n_2$, $t \equiv r \pmod{n_1}$ and $t \equiv s \pmod{n_2}$. Let $f(z)$ be the pseudo-random sequence of $\delta_m(4)$ corresponding to (A_{ij})—see Section IV.

i) Suppose t is such that the sequences $f(z)$, $z^t f(z)$, $z^{2t} f(z)$, $z^{3t} f(z)$ are linearly independent. If $m = 4$, these are a set of generators for the code $\delta_4(4)$. Therefore the columns of the array

$$f(z)$$
$$z^t f(z)$$
$$z^{2t} f(z)$$
$$z^{3t} f(z) \quad (42)$$

contain each of the 255 nonzero 4-tuples from the set $\{0, 1, \omega, \omega^2\}$ exactly once. Then

$$\tau(r, s) = \frac{1}{255} (\text{number of times } f_t \text{ is } 1, \omega \text{ or } \omega^2; f_{t+t} \text{ is } 0, \omega \text{ or } \omega^2; f_{t+2t} \text{ is } 0, 1 \text{ or } \omega^2; \text{ and } f_{t+3t} \text{ is } 0, 1 \text{ or } \omega)$$
$$= \frac{3^4}{255} = \frac{81}{255}.$$

If $m > 4$ then

$$\tau(r, s) = \frac{81 \cdot 4^{m-4}}{4^m - 1}. \quad (43)$$

To test whether these sequences are linearly independent we

map them into $GF(4^m)$ using the mapping given in Section II-K. Now

$$f(\xi^{-1}),\ \xi^{-t}f(\xi^{-1}),\ \xi^{-2t}f(\xi^{-1}),\ \xi^{-3t}f(\xi^{-1})$$

are linearly independent over $GF(4)$ if the equation

$$a_0 + a_1\delta + a_2\delta^2 + a_3\delta^3 = 0$$

where $\delta = \xi^{-t}$, $a_i \in GF(4)$, implies all $a_i = 0$. This means that the equation of least degree satisfied by δ over $GF(4)$ must have degree $\geqslant 4$. Most elements of $GF(4^m)$ satisfy a minimal equation of degree m (which is the reason for the condition $m \geqslant 4$). However, the elements 1, $\xi^{(4^m-1)/3}$ and $\xi^{2(4^m-1)/3}$ satisfy an equation of degree 1. If m is divisible by 2 or 3 there are also elements which satisfy equations of degree 2 or 3.

ii) Suppose $t = (4^m - 1)/3$. Then $z^t f(z) = \omega^{\pm 1} f(z)$, $z^{2t} f(z) = \omega^{\pm 2} f(z)$, and $z^{3t} f(z) = f(z)$. The columns of (42) are of one of the types

$$\begin{matrix} 0 & 1 & \omega & \omega^2 \\ 0 & \omega & \omega^2 & 1 \\ 0 & \omega^2 & 1 & \omega \\ 0 & 1 & \omega & \omega^2 \end{matrix} \quad \text{or} \quad \begin{matrix} 0 & 1 & \omega & \omega^2 \\ 0 & \omega^2 & 1 & \omega \\ 0 & \omega & \omega^2 & 1 \\ 0 & 1 & \omega & \omega^2 \end{matrix}$$

and $\tau(r, s) = 4^{m-1}/(4^m - 1)$ or 0, respectively. If m is prime, i) and ii) exhaust all the values of t. (If m is divisible by 2 or 3 other values of $\tau(r, s)$ can occur and can be found in the same way.) When $m = 4$, the transmission function $\tau(r, s)$ of Fig. 21 is given by

$$\tau(0, 0) = \tau(10, 0) = 0,\quad \tau(5, 0) = 0.502$$

$$\tau(r, 0) = 0.314 \text{ for } 1 \leqslant r \leqslant 14,\quad r \neq 5, 10$$

$$\tau(r, s) = 0.318 \text{ for all other pairs } (r, s) \text{ in}$$

$$\text{the range } 0 \leqslant r \leqslant 14,\quad 0 \leqslant s \leqslant 14. \quad (44)$$

VI. Summary

Pseudo-random sequences of 0's and 1's are constructed in Sections II-A and II-B; examples are shown in Fig. 7. They exist for all lengths of the form $n = 2^m - 1$, and their properties are discussed in Sections II-C through II-K. Properties I–IV, VI, and VII, are the most important.

Pseudo-random arrays of 0's and 1's of size $n_1 \times n_2$ exist whenever n_1 and n_2 are relatively prime, $n = n_1 n_2 = 2^{k_1 k_2} - 1$, and $n_1 = 2^{k_1} - 1$; examples are shown in Fig. 14. The construction is given in Section III-A and their properties in Sections III-B and III-C. Arrays with more general values of n_1 and n_2 are mentioned in Section III-D.

Pseudo-random sequences with entries from an alphabet of q symbols and length $q^m - 1$ are constructed in Seciton IV-A, examples are given in Fig. 20. These can also be formed into arrays, as illustrated in Fig. 21.

Section V discusses the transmission function (a kind of generalized autocorrelation function) of a set of binary arrays obtained from the pseudo-random sequences given in Section IV-A.

Appendix

Proof of the Window Property III:* Let α be a primitive element of $GF(2^{k_1 k_2})$. Let G be an $n \times k_1 k_2$ generator matrix for the simplex code $\mathcal{S}_{k_1 k_2}$ of length $n = 2^{k_1 k_2} - 1$, dimension $k_1 k_2$ and minimum distance $2^{k_1 k_2 - 1}$. The rows of G may be taken to be the binary $k_1 k_2$-tuples which are rectangular coordinates for the elements $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ of $GF(2^{k_1 k_2})$. Of course $\alpha^n = 1$. Let $I(i, j)$ be the unique integer satisfying

$$I(i, j) \equiv i \pmod{n_1}$$

$$I(i, j) \equiv j \pmod{n_2}$$

and

$$0 \leqslant I(i, j) \leqslant n - 1.$$

The window property will follow from the following result. *Theorem:* The rows of G which represent $\alpha^{I(i,j)}$ for $0 \leqslant i \leqslant k_1 - 1$ and $0 \leqslant j \leqslant k_2 - 1$ are linearly independent over $GF(2)$.

Proof: Suppose

$$\sum_{i=0}^{k_1-1} \sum_{j=0}^{k_2-1} c_{ij}\alpha^{I(i,j)} = 0, \qquad c_{ij} \in GF(2). \quad (45)$$

We must show that every $c_{ij} = 0$. Let Q denote the left-hand side of (45). With μ, ν as in (28) set $\beta = \alpha^{\nu n_2}$, $\gamma = \alpha^{\mu n_1}$. Then $\alpha = \beta\gamma$, $\alpha^{I(i,j)} = \beta^i \gamma^j$, and

$$Q = \sum_{j=0}^{k_2-1} \gamma^j \sum_{i=0}^{k_1-1} c_{ij}\beta^i.$$

Now n_1 and n_2 are the smallest positive integers such that $\beta^{n_1} = 1$, $\gamma^{n_2} = 1$. Since $n_1 = 2^{k_1} - 1$, $\beta \in GF(2^{k_1})$. Furthermore, β is a zero of an irreducible polynomial of degree k_1 over $GF(2)$, and of no polynomial of lower degree. The coefficient of γ^j in Q is an element of $GF(2^{k_1})$; hence it is necessary to find the lowest degree polynomial over $GF(2^{k_1})$ satisfied by γ. Let t be the least integer such that $\gamma^{2^t - 1} = 1$. Then $\alpha^{\mu n_1 (2^t - 1)} = 1$, so $\mu n_1 (2^t - 1)$ is divisible by $n_1 n_2$, and $2^t - 1$ is divisible by n_2. Now $n_2 = (2^{k_1 k_2} - 1)/(2^{k_1} - 1)$ has binary representation

$$1\overbrace{0\,0\cdots 0}^{k_1-1}1\overbrace{0\,0\cdots 0}^{k_1-1}1\cdots 1\overbrace{0\,0\cdots 0}^{k_1-1}1$$

with k_2 1's. The binary representation of $2^t - 1$ is $11\cdots 1$ with t 1's. Comparing these we see that the least t for which n_2 is divisible by $2^t - 1$ is $t = k_1 k_2$. Thus $t = k_1 k_2$ is the least positive integer such that $\gamma^{2^t} = \gamma$, and the k_2 elements

$$\gamma, \gamma^{2^{k_1}}, \gamma^{2^{2k_1}}, \cdots, \gamma^{2^{(k_2-1)k_1}}$$

are distinct. The polynomial of least degree satisfied by γ over $GF(2^{k_1})$ is

$$\prod_{i=0}^{k_2-1} (x - \gamma^{2^{ik_1}})$$

of degree k_2. Now Q is a polynomial of degree $k_2 - 1$ in γ with coefficients from $GF(2^{k_1})$. Thus $Q = 0$ implies

$$\sum_{i=0}^{k_1-1} c_{ij}\beta^i = 0, \qquad 0 \leqslant j \leqslant k_2 - 1.$$

But this is a polynomial of degree $k_1 - 1$, and β satisfies no equation of degree less than k_1. Therefore, $c_{ij} = 0$ for all i, j. Q.E.D.

Proof of the Window Property III:* Suppose the codewords $a(z)$ of $\mathcal{S}_{k_1 k_2}$ are folded into $n_1 \times n_2$ arrays $b(x, y)$ as in

Section III-A. From the theorem, the $k_1 \times k_2$ array in the North-West corner of $b(x, y)$ can be chosen arbitrarily, and determines the rest of the codeword. If W is a $k_1 \times k_2$ window placed in the North-West corner of $b(x, y)$, as $a(z)$ runs through the nonzero codewords of $\delta_{k_1 k_2}$ W sees each nonzero $k_1 \times k_2$ array once. If $b(x, y) \neq 0$, the arrays consist of all $x^i y^j b(x, y)$. Since the view of $x^i y^j b(x, y)$ seen by W is the same as the view of $b(x, y)$ seen by $x^{-i} y^{-j} W$, this proves the window property. Q.E.D.

Acknowledgment

We should like to thank Ken Knowlton for telling us about the physical problem [43] which stimulated this research, and Allen Gersho for helping to translate the physical problem into a nice mathematical one.

References

[1] J. D. Alanen and D. E. Knuth, "Tables of finite fields," *Sankhyā*, Series A, vol. 26, pp. 305–328, 1964.
[2] J. R. Ball, A. H. Spittle, and H. T. Liu, "High-speed m-sequence generation: a further note," *Electron. Lett.*, vol. 11, pp. 107–108, 1975.
[3] C. Balza, A. Fromageot, and M. Maniere, "Four-level pseudo-random sequences," *Electron. Lett.*, vol. 3, pp. 313–315, 1967.
[4] T. C. Bartee and D. I. Schneider, "Computation with finite fields," *Infom. Contr.*, vol. 6, pp. 79–98, 1963.
[5] L. D. Baumert, "Cyclic Hadamard matrices," *JPL Space Programs Summary*, vol. 37-43-IV, pp. 311–314 and 338, 1967.
[6] J. T. B. Beard, Jr., "Computing in GF(q)," *Math. Comput.*, vol. 28, pp. 1159–1166, 1974.
[7] J. T. B. Beard, Jr., and K. I. West, "Some primitive polynomials of the third kind," *Math. Comput.*, vol. 28, pp. 1166–1167, 1974.
[8] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[9] ——, "Some mathematical properties of a scheme for reducing the bandwidth of motion pictures by Hadamard smearing," *Bell Syst. Tech. J.*, vol. 49, pp. 969–986, 1970.
[10] E. R. Berlekamp and J. Justesen, "Some long cyclic linear binary codes are not so bad," *IEEE Trans. Inform. Theory*, vol. 20, pp. 351–356, 1974.
[11] P. A. N. Briggs and K. R. Godfrey, "Autocorrelation function of a 4-level m-sequence," *Electron. Lett.*, vol. 4, 232–233, 1963.
[11a] N. G. de Bruijn, "A combinatorial problem," *Nederl. Akad. Wetensch. Proc. Ser. A.*, vol. 49, pp. 758–764, 1946-*Indag. Math.*, vol. 8, pp. 461–467, 1946.
[12] D. Calabro and J. K. Wolf, "On the synthesis of two-dimensional arrays with desirable correlation properties," *Imform. Contr.*, vol. 11, pp. 537–560, 1968.
[13] D. E. Carter, "On the generation of pseudo-noise codes," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 10, pp. 898–899, 1974.
[14] J. A. Chang, "Generation of 5-level maximal-length sequences," *Electron. Lett.*, vol. 2, p. 258, 1966.
[15] J. H. Conway, "A tabulation of some information concerning finite fields," *Computers in Mathematical Research*, R. F. Churchhouse and J. C. Herz, Eds. Amsterdam: North-Holland, 1968, pp. 37–50.
[16] I. G. Cumming, "Autocorrelation function and spectrum of a filtered, pseudo-random binary sequence," *Proc. Inst. Elec. Eng.* vol. 114, pp. 1360–1362, 1967.
[17] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Univ. Maryland, College Park. 1974.
[17a] J. V. Evans and T. Hagfors, Eds., *Radar Astronomy*. New York: McGraw-Hill, 1968.
[18] H. Feistel, W. A. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," *Proc. IEEE*, vol. 63, pp. 1545–1554, 1975.
[19] J. P. Fillmore and M. L. Marx, "Linear recursive sequences," *SIAM Review*, vol. 10, pp. 342–353, 1968.
[19a] H. Fredricksen, "The lexicographically least de Bruijn cycle," *J. Combinatorial Theory*, vol. 9, pp. 1–5, 1970.
[19b] H. Fredricksen, "A class of nonlinear de Bruijn cycles," *J. Combinatorial Theory*, vol. 19A, pp. 192–199, 1975.
[20] S. Fredricsson, "Pseudo-randomness properties of binary shift register sequences," *IEEE Trans. Inform. Theory*, vol. 21, pp. 115–120, 1975.
[21] P. R. Geffe, "An open letter to communication engineers," *Proc. IEEE*, vol. 55, p. 2173, 1967.
[22] ——, "How to protect data with ciphers that are really hard to break," *Electronics*, vol. 46, pp. 99–101, Jan. 1973.
[23] E. N. Gilbert, unpublished.
[24] A. Gill, *Linear Sequential Circuits*. New York: McGraw-Hill, 1966.
[25] K. R. Godfrey, "Three-level m-sequences," *Electron. Lett.*, vol. 2, pp. 241–243, 1966.
[26] J. -M. Goethals, Factorization of cyclic codes, *IEEE Trans. Inform. Theory*, vol. 13, pp. 242–246, 1967.
[27] R. Gold, Characteristic linear sequences and their coset functions, *SIAM J. Appl. Math.*, vol. 14, pp. 980–985, 1966.
[28] S. W. Golomb, Ed., *Digital Communications with Space Applications*. Englewood Cliffs, N.J.,: Prentice-Hall, 1964.
[29] S. W. Golomb, *Shift Register Sequences*. San Francisco: Holden-Day, 1967.
[30] B. Gordon, "On the existence of perfect maps," *IEEE Trans. Inform. Theory*, vol. 12, pp. 486–487, 1966.
[31] D. Gorenstein and E. Weiss, "An acquirable code," *Inform. Contr.*, vol. 7, pp. 315–319, 1964.
[32] D. H. Green and I. S. Taylor, "Irreducible polynomials over composite Galois fields and their applications in coding techniques," *Proc. Inst. Elec. Eng.*, vol. 121, pp. 935–939, 1974.
[33] R. R. Green, "A serial orthogonal decoder," *JPL Space Programs Summary*, vol. 37-39-IV, pp. 247–253, 1966.
[34] ——, "Analysis of a serial orthogonal decoder," *JPL Space Programs Summary*, vol. 37-53-III, pp. 185–187, 1968.
[35] M. Hall, Jr., *Combinatorial Theory*. Waltham, MA: Blaisdell, 1967.
[36] J. T. Harvey, "High-speed m-sequence generation," *Electron. Lett.*, vol. 10, pp. 480–481, 1974.
[37] M. Harwit, "Spectrometric imager," Applied Optics, vol. 10, pp. 1415–1421, 1971, and vol. 12, pp. 285–288, 1973.
[38] ——, private communication.
[39] U. Henriksson, "On a scrambling property of feedback shift registers," *IEEE Trans. Commun.*, vol. 20, pp. 998–1001, 1972.
[40] T. Ikai and Y. Kojima," Two-dimensional cyclic codes," *Electron. Commun. in Japan*, vol. 57-A, pp. 27–35, 1974.
[41] H. Imai, "Two-dimensional Fire codes," *IEEE Trans. Inform. Theory*, Vol. 19, pp. 796–806, 1973.
[42] W. H. Kautz, Ed., *Linear Sequential Switching Circuits: Selected Papers*. San Francisco: Holden-Day, 1965.
[43] K. Knowlton, private communication.
[43a] D. E. Knuth, *The Art of Computer Programming*. Reading, MA.: Addison-Wesley, 1968, vol. 1, p. 379.
[43b] Y. I. Kotov, "Correlation function of composite sequences constructed from two M-sequences," *Radio Eng. Electron. Phys.*, vol. 19, pp. 128–130, 1974.
[43c] J. Lindner, "Binary sequences up to length 40 with best possible autocorrelation function," *Electron. Lett.*, vol. 11, p. 507, 1975.
[44]. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland Publishing, to appear.
[45] R. L. McFarland, "A family of difference sets in noncyclic groups," *J. Combinatorial Theory*, vol. 15A, pp. 1–10, 1973.
[46] K. Nakamura and Y. Iwadare, "Data Scramblers for multilevel pulse sequences," *NEC Research and Development*, No. 26, pp. 53–63, July 1972.
[47] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*. New York: Wiley, 1966, 2nd edition.
[48] T. Nomura and A. Fukuda, "Linear recurring planes and two-dimensional cyclic codes," *Electron. Commun. in Japan*, vol. 54A, pp. 23–30, 1971.
[49] T. Nomura, H. Miyakawa, H. Imai, and A. Fukuda, "A method of construction and some properties of planes having maximum area matrix," *Electron. Commun. in Japan*, vol. 54A, pp. 18–25, 1971.
[50] ——, "Some properties of the $\gamma\beta$-plane and its extension to three-dimensional space," *Electron. Commun. in Japan*, vol. 54A, pp. 27–34, 1971.
[51] ——, "A Theory of two-dimensional linear recurring arrays," *IEEE Trans. Inform. Theory*, vol. 18, pp. 775–785, 1972.
[52] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*. Cambridge, MA: M. I. T. Press, 1972, 2nd ed.
[52a] G. H. Pettengill, Radar Handbook, M. I. Skolnik, Ed. New York: McGraw-Hill, 1970, Ch. 33.
[53] E. C. Posner, "Combinatorial Structures" in *Planetary Reconnaissance, in Error Correcting Codes*, H. B. Mann, Ed. New York: Wiley, 1969, pp. 15–46.
[54] I. S. Reed and R. M. Stewart, "Note on the existence of perfect maps," *IEEE Trans. Inform. Theory*, vol. 8, pp. 10–12, 1962.
[55] P. D. Roberts and R. H. Davis, "Statistical properties of smoothed maximal-length linear binary sequences," *Proc. Inst. Elec. Eng.*, vol. 113, pp. 190–196, 1966.
[56] O. S. Rothaus, "On 'Bent' Functions," *J. Combinatorial Theory*, vol. 20A, pp. 300–305, 1976.
[57] J. E. Savage, "Some simple self-synchronizing digital data scramblers," *Bell Syst. Tech. J.*, vol. 46, pp. 449–487, 1967.
[58] P. H. R. Scholefield, "Shift registers generating maximum-length sequences," *Electron. Technol.*, vol. 37, pp. 389–394, 1960.
[59] M. R. Schroeder, "Sound diffusion by maximum-length se-

quences," *J. Acoust. Soc. Am.*, vol. 57, pp. 149-150, 1975.
[60] E. S. Selmer, "Linear recurrence relations over finite fields," Dept. of Math., Univ. of Bergen, Norway, 1966.
[61] N. J. A. Sloane, T. Fine, P. G. Phillips, and M. Harwit, "Codes for Multislit Spectrometry," *Appl. Opt.*, vol. 8, pp. 2103-2106, 1969.
[62] N. J. A. Sloane and M. Harwit, "Masks for Hadamard transform optics, and weighing designs," *Appl. Opt.*, vol. 15, pp. 107-114, 1976.
[63] R. Spann, "A Two-Dimensional correlation property of pseudo-random maximal-length sequences," *Proc. IEEE*, vol. 53, p. 2137, 1963.
[64] W. Stahnke, "Primitive binary polynomials," *Math. Comput.*, vol. 27, pp. 977-980, 1973.
[65] J. J. Stiffler, *Theory of Synchronous Communications*. Englewood Cliffs, NS: Prentice-Hall, 1971.
[66] M. H. Tai, M. Harwit, and N. J. A. Sloane, "Errors in Hadamard spectroscopy or imaging caused by imperfect masks," *Appl. Opt., vol. 14, pp.* 2678-2686, 1975.
[67] R. Theone and S. W. Golomb, "Search for cyclic Hadamard matrices," *JPL Space Programs Summary*, vol. 37-40-IV, pp. 207-208, 1966.
[67a] S. A. Tretter, "Properties of PN^2 sequences," *IEEE Trans. Inform. Theory*, vol. 20, pp. 295-297, 1974.
[68] S. H. Tsao, "Generation of delayed replicas of maximal-length linear binary sequences," *Proc. Inst. Elec. Eng.*, vol. 111, pp. 1803-1806, 1964.
[69] R. Turyn, "Sequences with small correlation," in *Error Correcting Codes*, H. B. Mann, Ed. New York: Wiley, 1969, pp. 195-228.
[70] J. V. Uspensky and M. A. Heaslet, *Elementary Number Theory*. New York: McGraw-Hill, 1939.
[71] W. D. Wallis, A. P. Street, and J. S. Wallis, "Combinatorics: Room squares, sum-free sets, Hadamard matrices," *Lecture Notes in Mathematics 292*. Berlin: Springer, 1972.
[72] G. D. Weathers, E. R. Graf, and G. R. Wallace, "The subsequence weight distribution of summed maximum length digital sequences," *IEEE Trans. Commun.*, vol. 22, pp., 997-1004, 1974.
[73] L. R. Welch, "Computation of finite Fourier series," *JPL Space Programs Summary*, vol. 37-37-IV, pp. 295-297, 1966.
[74] L. -J. Weng, "Decomposition of M-sequences and its applications," *IEEE Trans. Inform. Theory*, vol. 17, pp. 457-463, 1971.
[75] M. Willett, "The index of an m-sequence," *SIAM J. Appl. Math.*, vol. 25, pp. 24-27, 1973.
[76] N. Zierler, "Linear recurring sequences," *J. Soc. Ind. Appl. Math.*, vol. 7, pp. 31-48, 1959.
[77] ——, "Linear recurring sequences and error-correcting codes," *Error Correcting Codes*, H. B. Mann, Ed., New York: Wiley, 1969, pp. 47-59.
[78] N. Zierler and J. Brillhart, "On primitive trinomials (mod 2)," *Inform. Cont.*, vol. 13, pp. 541-554, 1968, and vol. 14, pp. 566-569, 1969.

Contributors

F. A. Benson (M'50-SM'62-F'75) was educated at the University of Liverpool, Liverpool, England, where he received the degrees of B. Eng. and M. Eng. He has also been awarded the degrees of Ph.D. and D. Eng. by the University of Sheffield, Sheffield, England.

After serving as a Member of the Research Staff at the Admiralty Signal Establishment, Witley, England, during the World War II, he became an Assistant Lecturer in Electrical Engineering at the University of Liverpool. Since 1949, he has been on the Staff at the University of Sheffield, first as a Lecturer, then as a Senior Lecturer, and later Reader in Electronics. He became Professor and Head of the Department of Electronic and Electrical Engineering in 1967. He has been a Pro-Vice-Chancellor in the University of Sheffield since 1972.

*

Chak Ming Chie (S'75) was born in Hong Kong, on August 29, 1951. He received the B.S.E.E. and B.A. (Math) degree from the University of Minnesota, MN, in 1972, and the M.S. degree in electrical engineering from the University of Southern California (USC), Los Angeles, in 1974.

From 1972 to 1974, he was a Teaching Assistant at USC. He is presently a Research Assistant working for a Ph.D. degree at USC with major interest in the synchronization aspect of digital communication systems.

Charles Elachi (M'71) was born in Rayak, Lebanon, on April 18, 1947. He received the "ingenieur" degree in radioelectricity with honors and the "Prix de la Houille Blanche" from the Polytechnic Institute of Grenoble, France, in 1968, and the M.S. and Ph.D. degrees in electrical engineering and business economics from the California Institute of Technology, Pasadena, in 1969 and 1971, respectively.

He has worked at the Physical Spectrometry Laboratory, University of Grenoble, France, on plasma in microwave cavities. He was a Teaching Assistant at Caltech in 1969. In 1970 he joined the Space Sciences Division, Jet Propulsion Laboratory, Pasadena, where he is presently Surpervisor of the Radar Science and Applications Group which is involved in investigating spacecraft borne scientific experiments for planetary and Earth studies using coherent radar techniques. He is a Principal Investigator on the Lunar Data Analysis and Synthesis Program. He is also involved in studying theoretical electromagnetic problems related to stratified media, space-time periodic media and DFB lasers. He is also affiliated with the University of California, Los Angeles. He has 60 papers, patents, reports, and conference presentations in the above fields.

In 1973, Dr. Elachi was the first recipient of the R. W. P. King award. He is a member of the Optical Society of America, AAAS and Sigma Xi.

*

Reuben Hackam received the B.Sc. degree from the Technion–Israel Institute of Technology, Haifa, Israel, in 1960, and the Ph.D. degree from the University of Liverpool, Liverpool, England in 1964.