On pseudo-random arrays

SIAM J. APPL. MATH.
Vol. 36, No. 1, February, 1979

0036-1399/79/3601-0006 $01.00/0

ON PSEUDO-RANDOM ARRAYS*

J. H. VAN LINT,† F. J. MACWILLIAMS‡ AND N. J. A. SLOANE‡

Abstract. An arrays of 0's and 1's has the $u \times v$ horizontal window property if every nonzero view is seen once when a $u \times v$ window is moved horizontally across the array. We study the problem of constructing an array which, for a given m, has the $u \times v$ horizontal window property for all factorizations $m = uv$. Using maximal linear shift register sequences for the rows we are able to construct such arrays of size $m \times (2^m - 1)$ for various values of m, including all $m \leqq 34$ and $m = p$ or p^2 where p is prime. Similarly we construct arrays of size $(2^m - 1) \times (2^m - 1)$ which have both the $u \times v$ horizontal window property and the $u \times v$ vertical window property for all factorizations $m = uv$.

1. Introduction. Pseudo-random sequences and arrays have been studied by many authors (see [1]–[19]). However the problem discussed in this paper seems to be new. An array of 0's and 1's is said to have the $u \times v$ *horizontal window property* if every nonzero view is seen once when a $u \times v$ window is moved horizontally across the array. (To avoid trouble at the ends, the array should be imagined as being written on a vertical cylinder.) Similarly the $u \times v$ *vertical window property* holds if every nonzero view appears once when the window is moved vertically down the array (and the array is imagined to be written on a horizontal cylinder).

We are interested in the following questions. Problem (I). Given m, does there exist a $(2^m - 1) \times (2^m - 1)$ array which has both the $u \times v$ horizontal and vertical window properties for every factorization $m = uv$? An easier question is: Problem (II). Given m, does there exist an $m \times (2^m - 1)$ array which has the $u \times v$ horizontal window property for every factorization $m = uv$? These problems arose from a discussion with M. R. Schroeder concerning the design of experiments in acoustics.

The following simple construction solves these problems in many cases. Let $h(x)$ be a primitive binary polynomial of degree m, and let $\mathbf{a} = a_0, a_1, \cdots, a_{2^m-2}$ be the corresponding maximal length shift register sequence of length $2^m - 1$ [15], [13]. The array has first row $\mathbf{a}$, and subsequent rows are obtained by cyclically shifting the previous row s places to the right. We take either $2^m - 1$ rows to get a solution to Problem (I), or only m rows to solve Problem (II). Examples are given in Figs. 1(b), 2 and 3. Not every s works, and in at least one case no s works—if $h(x)$ is the primitive polynomial $x^6 + x^5 + x^3 + x^2 + 1$ then there is no value of s for which the array is a solution to Problem (I) or (II). However we conjecture that for every m there is a primitive polynomial $h(x)$ and a suitable shift s for which our construction solves both problems.

2. Construction and properties of the arrays. In this section we construct the arrays and investigate which window properties hold. Let $h(x) = x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + h_0$ be a primitive binary polynomial, where $h_0 = 1$. The maximal length shift register sequence $\mathbf{a}$ corresponding to $h(x)$ is the sequence

$$\mathbf{a} = a_0, a_1, \cdots, a_{2^m-2} \tag{1}$$

where

$$a_0 = a_1 = \cdots = a_{m-2} = 0, \qquad a_{m-1} = 1 \tag{2}$$

* Received by the editors December 2, 1977.

† Bell Laboratories, Murray Hill, New Jersey 07974. Permanent address: Technological University of Eindhoven, Eindhoven, The Netherlands.

‡ Bell Laboratories, Murray Hill, New Jersey 07974.

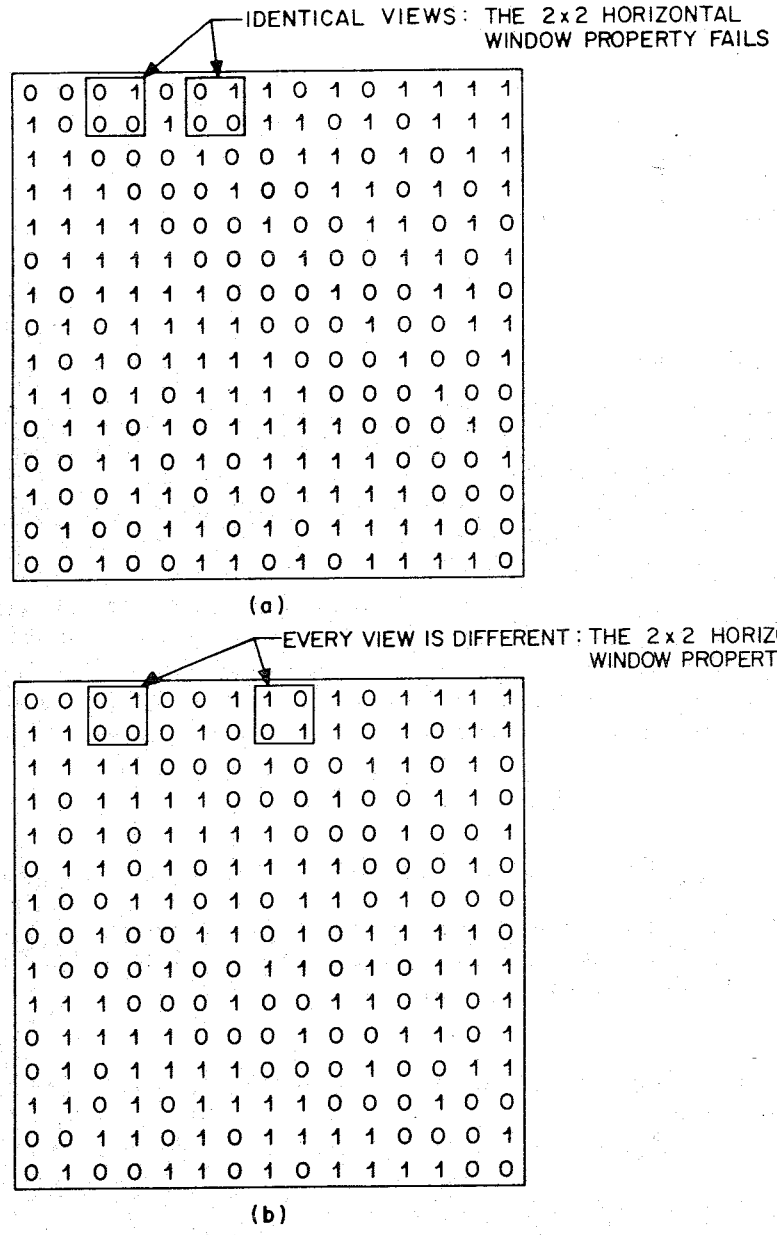

FIG. 1 (a) *The array* $M(x^4+x+1, 1)$, *which has the* 4×1 *and* 1×4 *window properties, but not the* 2×2 *horizontal or vertical window property* $\left(\text{e.g. } \begin{matrix}01\\00\end{matrix} \text{ appears twice in the first two rows}\right)$. (b) *The array* $M(x^4+x+1, 2)$, *which has all* 4×1, 2×2 *and* 1×4 *horizontal and vertical window properties.*

and

$$a_{r+m} = h_{m-1}a_{r+m-1} + \cdots + h_0 a_r, \tag{3}$$

$r = 0, 1, \cdots$. The set of all binary polynomials taken modulo $h(x)$ is a representation of the field $GF(2^m)$ [20], [21]. The polynomial x will be denoted by α, so that $h(\alpha)=0$. If

$$x^i \equiv c_{i,m-1}x^{m-1} + \cdots + c_{i,0}x^0 \pmod{h(x)} \tag{4}$$

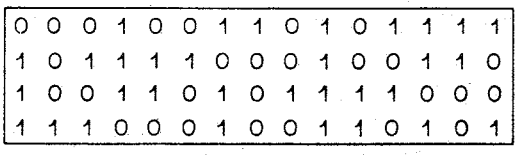

FIG. 2. *The array* $M_0(x^4+x+1, 6)$, *which has all* 4×1, 2×2 *and* 1×4 *horizontal window properties.*

where the coefficients $c_{j,i}$ are 0 or 1, then

$$a_j = c_{j,m-1}a_{m-1}+\cdots+c_{j,0}a_0 \tag{5}$$

$$= c_{j,m-1} \tag{6}$$

because of the initial conditions (2).

Construction of the arrays $M(h, s)$ and $M_0(h, s)$. Let s be an integer in the range $1 \leqq s \leqq 2^m-2$. The $(2^m-1)\times(2^m-1)$ array $M(h, s)$ has first row **a** and subsequent rows are obtained by cyclically shifting the previous row s places to the right. Then $M_0(h, s)$ consists of the first m rows of $M(h, s)$. We shall see that in many (perhaps all) cases it is possible to choose $h(x)$ and s so that $M(h, s)$ is a solution to Problem (I), or so that $M_0(h, s)$ is a solution to Problem (II). (See Tables 1 and 2.)

Examples. For $m=4$, $h(x)=x^4+x+1$, the arrays $M(x^4+x+1, 1)$ and $M(x^4+x+1, 2)$ are shown in Figs. 1(a) and (b), and $M_0(x^4+x+1, 6)$ in Fig. 3. Note that in Fig. 1(b), $M(x^4+x+1, 2)$ has the 4×1, 2×2 and 1×4 horizontal and vertical window properties and is therefore a solution to Problem (I). For example, the 2×2 horizontal window property holds because in any two adjacent rows, say the first two, each of

$$00,\ 00,\ \ldots,\ 11$$
$$01,\ 10,\ \ldots,\ 11$$

appears exactly once. $\left(\begin{smallmatrix}10\\11\end{smallmatrix}\right.$ is found in the last column followed by the first.$\left.\right)$ On the other hand, in Fig. 1(a), $M(x^4+x+1, 1)$ has the 4×1 and 1×4 window properties but not the 2×2 horizontal or vertical window property. A larger example is shown in Fig. 3.

It is clear that the first column of $M(h, s)$ is

$$a_0, a_{-s}, a_{-2s}, \cdots \tag{7}$$

with subscripts taken modulo 2^m-1, i.e. it is formed by taking every (2^m-1-s)-th term of the infinite sequence $a_0, a_1, \cdots$. If g.c.d. $(s, 2^m-1)\neq1$, then $M(h, s)$ has repeated rows and cannot be a solution to Problem (I), even though the first m rows

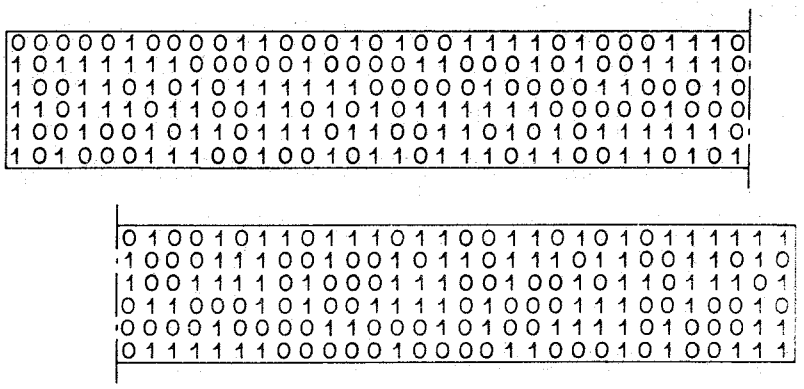

FIG. 3. *The array* $M_0(x^6+x+1, 8)$, *which has all* 6×1, 3×2, 2×3 *and* 1×6 *horizontal window properties.*

TABLE 1

For each composite $m \leqq 34$ the table gives one or two primitive polynomials $h(x)$. s_I = smallest s for which $M(h, s_I)$ is a solution to Problem (I), *and s_{II} = smallest s for which $M(h, s_{II})$ is a solution to Problem* (II).

m	$h(x)$	s_I	s_{II}
4	x^4+x+1	2†	2†
6	$x^6+x^5+x^2+x+1$	8§	3†
8	$x^8+x^7+x^6+x^5+x^2+x+1$	4†	4†
9	x^9+x^4+1	3†	3†
10	$x^{10}+x^8+x^6+x^4+x^2+x+1$	5†	5†
12	$x^{12}+x^{10}+x^9+x^6+x^2+x+1$	31	6†
	$x^{12}+x^{11}+x^9+x^8+x^7+x^5+x^2+x+1$	16§	16
14	$x^{14}+x^5+x^3+x+1$	7†	7†
15	$x^{15}+x^7+x^4+x+1$	5†	5†
16	$x^{16}+x^7+x^5+x^4+x^3+x^2+1$	8†	8†
18	$x^{18}+x^{12}+x^6+x^4+x^3+x+1$	94	9†
	$x^{18}+x^{10}+x^9+x^8+x^5+x^4+1$	10§	10
20	$x^{20}+x^6+x^4+x+1$	116	10§
	$x^{20}+x^{10}+x^9+x^6+x^5+x^4+x^3+1$	13§	13
21	$x^{21}+x^2+1$	26	26
22	$x^{22}+x+1$	74	74
24	$x^{24}+x^4+x^3+x+1$	1433	87
25	$x^{25}+x^3+1$	5†	5†
26	$x^{26}+x^8+x^7+x+1$	13†	13†
27	$x^{27}+x^8+x^7+x+1$	9†	9†
28	$x^{28}+x^{13}+1$	68	68
30	$x^{30}+x^6+x^4+x+1$		334
32	$x^{32}+x^{28}+x^{27}+x+1$	122	69
33	$x^{33}+x^6+x^4+x+1$	22	22
34	$x^{34}+x^{15}+x^{14}+x+1$	17†	17†

† Meets the bounds (11).
§ Minimum s_I for the value of m.

alone may solve Problem (II). On the other hand, if g.c.d. $(s, 2^m-1)=1$, then each column of $M(h, s)$ is obtained by cyclically shifting the previous column t places downwards, where $st \equiv 1 \pmod{2^m-1}$.

Tables of $h(x)$ and **a** are readily available in the literature [6], [13], [22]–[31] and so the arrays $M(h, s)$ and $M_0(h, s)$ are easily computed.

The following theorem makes it possible to test whether or not $M(h, s)$ or $M_0(h, s)$ has a particular window property.

THEOREM 1. *The following three statements are equivalent.*

(i) *$M(h, s)$ or $M_0(h, s)$ has the $u \times v$ horizontal window property.*

(ii) *No linear combination of*

$$1, x, x^2, \cdots, x^{v-1};\quad x^s, x^{s+1}, \cdots, x^{s+v-1};\quad x^{2s}, \cdots;\quad x^{(u-1)s+1}, \cdots, x^{(u-1)s+v-1} \tag{8}$$

with coefficients 0 and 1 is divisible by $h(x)$.

(iii) *The elements*

$$1, \alpha, \alpha^2, \cdots, \alpha^{v-1};\quad \alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+v-1};\quad \alpha^{2s}, \cdots;\quad \alpha^{(u-1)s+1}, \cdots, \alpha^{(u-1)s+v-1} \tag{9}$$

of $GF(2^m)$ are linearly independent over $GF(2)$.

TABLE 2

For various m and $h(x)$ the table gives (unstarred) all values of s for which $M(h, s)$ has all possible horizontal and vertical window properties and $M_0(h, s)$ has all possible horizontal window properties. If s is starred then $M_0(h, s)$ has all possible horizontal window properties even though g.c.d.$(s, 2^m - 1) > 1$. The last two columns give the total number of s for which *$M(h, s)$ is a solution to Problem* (I) $(N_{\mathrm{I}}(h))$, *or for which $M_0(h, s)$ is a solution to Problem* (II) $(N_{\mathrm{II}}(h))$.

m, $h(x)$	Acceptable s for both Problems (unstarred) or Problem (II) only (starred)	$N_{\mathrm{I}}(h)$	$N_{\mathrm{II}}(h)$
$m=3$ $h(x)=x^3+x+1$	1, 2, 3, 4, 5, 6.	6	6
$m=4$ $h(x)=x^4+x+1$	2, 6*, 7, 8, 9*, 13.	4	6
$m=5$ $h(x)=x^5+x^2+1$	1, 2, 3, $\cdots$, 30.	30	30
$m=6$ $h(x)=x^6+x^5+x^2+x+1$	3*, 8, 11, 52, 55, 60*.	4	6
$m=6$ $h(x)=x^6+x+1$	8, 15*, 23, 40, 48*, 55.	4	6
$m=8$ $h(x)=x^8+x^7+x^6+x^5+x^2+x+1$	4, 8, 15*, 16, 18*, 23, 32, 35*, 37, 39*, 41, 42*, 44, 49, 50*, 52, 54*, 55*, 62, 64, 65*, 67, 73, 76, 77, 78*, 86, 99*, 100*, 106, 108*, 110*, 118 then 255-s.	38	66
$m=9$ $h(x)=x^9+x^4+1$	3, 6, 17, 22, 25, 26, 29, 31, 33, 34, 35*, 38, 43, 47, 48, 50, 55, 56*, 58, 62, $\cdots$	150	186
$m=10$ $h(x)=x^{10}+x^8+x^6+x^4+x^2+x+1$	5, 7, 14, 15*, 18*, 21*, 22*, 23, 28, 32, 37, 49, 50, 53, 65, 67, 68, 74, 86, 95, $\cdots$	162	252
$m=12$ $h(x)=x^{12}+x^{10}+x^9+x^6+x^2+x+1$	6*, 31, 46, 60*, 64, 153*, 186*, 225*, 285*, 327*, 353, 436, 464, 471*, 477*, 480*, 516*, 531*, 621*, 622, $\cdots$	58	132

Remark. A similar result holds for windows of irregular shape, e.g. 

Proof. (ii)$\Rightarrow$(i). Suppose two $u \times v$ subarrays of $M(h, s)$ are equal. Thus for some values of i and j

$$a_{i-ks-t} = a_{j-ks+t}$$

for all $0 \leqq k \leqq u-1$, $0 \leqq t \leqq v-1$. Hence by (4)–(6) the m polynomials

$$x^{i-ks+t} - x^{j-ks+t} \pmod{h(x)}$$

have degree $\leqq m-2$, and are therefore linearly dependent over $GF(2)$. Since

$$\text{g.c.d.}(x^{i-(u-1)s} - x^{j-(u-1)s}, h(x)) = 1,$$

we find that the polynomials (8) are linearly dependent modulo $h(x)$.

(i)$\Rightarrow$(ii). Conversely, suppose the polynomials (8) are linearly dependent modulo $h(x)$, say

$$\sum_{k=0}^{u-1}\sum_{t=0}^{v-1} d_{kt}x^{ks+t} \equiv 0 (\text{mod } h(x)), \tag{10}$$

where the coefficients d_{kt} are 0 or 1 and are not all zero. Therefore, for any i,

$$\sum_{k=0}^{u-1}\sum_{t=0}^{v-1} d_{kt}x^{i-ks+t} \equiv 0 (\text{mod } h(x)).$$

By examining the coefficient of x^{m-1} in this equation, and using (6), it follows that

$$\sum_{k=0}^{u-1}\sum_{t=0}^{v-1} d_{kt}a_{j-ks+t} = 0.$$

Hence the subarray

$$\begin{matrix} a_i & a_{i+1} & \cdots & a_{i+v-1} \\ a_{i-s} & a_{i-s+1} & \cdots & a_{i-s+v-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_{i-(u-1)s} & \cdots & \cdots & a_{i-(u-1)s+v-1} \end{matrix}$$

of $M(h, s)$ or $M_0(h, s)$ satisfies a linear constraint, and cannot take on all $2^{uv}-1$ different values as i varies. Therefore the $u \times v$ window property does not hold. (E.g. in Fig. 1(a) any 2×2 subarray has a constant main diagonal.)

(ii)$\Leftrightarrow$(iii). This is simply a translation of the statement that (10) holds if and only if

$$\sum_{k=0}^{u-1}\sum_{t=0}^{v-1} d_{kt}\alpha^{ks+t} = 0. \qquad \text{Q.E.D.}$$

Obviously if $M(h, s)$ (or $M_0(h, s)$) has a certain window property then so does $M(h, 2^m-1-s)$ (or $M_0(h, 2^m-1-s)$).

COROLLARY 2. *The $m \times 1$ horizontal window property holds for $M(h, s)$ or $M_0(h, s)$ if and only if the minimal polynomial* ([20], [21]) *of α^s has degree m.*

For example $M_0(x^4+x+1, 6)$ (see Fig. 2) has the 4×1 horizontal window property, and the minimal polynomial of α^6 is $x^4+x^3+x^2+x+1$.

THEOREM 3. *Suppose g.c.d.$(s, 2^m-1)=1$. Then the $u \times v$ vertical window property holds for $M(h, s)$ if and only if the $u \times v$ horizontal window property holds.*

Proof. Since g.c.d.$(s, 2^m-1)=1$ the first column (see (7)) is a maximal linear shift register sequence. Suppose the $u \times v$ horizontal window property holds but the $u \times v$ vertical window property does not. Without loss of generality we may assume that two identical windows appear in the first s columns. But (see Fig. 4) this implies that two identical windows appear in the first u rows. Q.E.D.

Thus if m is a prime, and $h(x)$ is any primitive polynomial of degree m, $M(h, 1)$ is a solution to Problem (I), and $M_0(h, 1)$ is a solution to Problem (II).

Another consequence of Theorem 1 is:

THEOREM 4. *If $M_0(h, s)$ is a solution to Problem (II) then*

$$s \geqq \textit{largest divisor of } m \textit{ which is less than } m. \tag{11}$$

Proof. If $m = uv$ and $s < v$ then the elements (9) are certainly not independent. Q.E.D.

Of course this bound is not always met. For example if $m = 6$, $h(x) = x^6+x+1$ then the smallest s is 8 (see Table 2). But we conjecture that for each m there exists an $h(x)$ such that, if s is the largest divisor of m less than m, then $M_0(h, s)$ is a solution to Problem (II). Table 1 shows the best results known to us. We have already observed that if m is prime s can be taken to be 1. For composite values of $m \leqq 34$ the table gives one

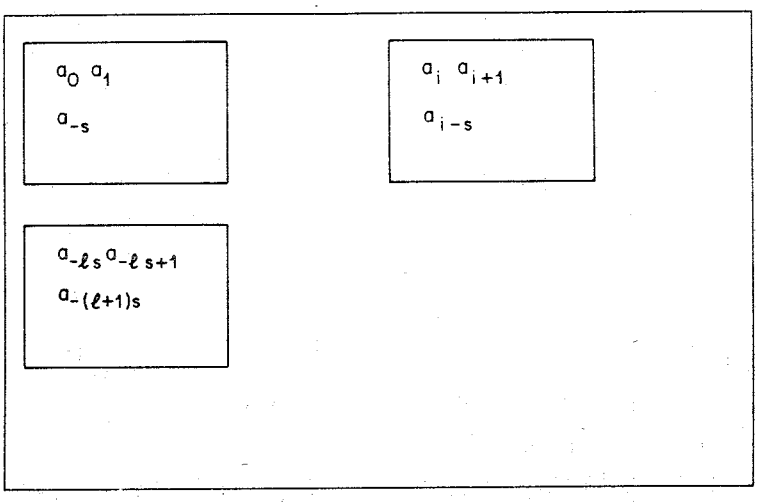

FIG.4. *The proof of Theorem* 3. *If* $-ls \equiv i \pmod{2^m-1}$ *then the three windows are equal.*

or two primitive polynomials $h(x)$ together with

s_I = smallest value of s for which $M(h, s_I)$ is a solution to Problem (I),

and

s_{II} = smallest value of s for which $M_0(h, s_{II})$ is a solution to Problem (II).

For $m \leqq 20$ the values of s_I and s_{II} in the table are the lowest possible for any choice of $h(x)$. The above conjecture is seen to hold for $m \leqq 20$ and some higher values. For $m > 20$ we have not carried out a systematic search for good $h(x)$.

THEOREM 5. *If* $m = uv$ *then* $M(h, u)$ *and* $M_0(h, u)$ *have the* $u \times v$ *horizontal window property.*

Proof. With this choice of s the elements (9) become $1, \alpha, \cdots, \alpha^{m-1}$, and are linearly independent by definition. Q.E.D.

COROLLARY 6. *If* $m = p^2$ (p *prime*) *then* $M(h, p)$ *is a solution to Problem* (*I*), *and* $M_0(h, p)$ *is a solution to Problem* (*II*).

Proof. In this case the only windows to be considered are of sizes $p^2 \times 1$, $p \times p$ and $1 \times p^2$. Q.E.D.

If $m = 2n$ the number of values of s for which the $2 \times n$ horizontal window property holds for $M(h, s)$ or $M_0(h, s)$ is, by Theorem 1, the number of s such that

$$f(\alpha) + \alpha^s g(\alpha) \neq 0$$

for all nonzero binary polynomials $f(x)$ and $g(x)$ of degree $\leqq n-1$. This number is clearly equal to $(2^{2n}-1)$ minus the number of pairs $(f(x), g(x))$ which are relatively prime.

THEOREM 7. *The number of pairs* $(f(x), g(x))$ *of nonzero binary polynomials of degree* $\leqq K$ *which are relatively prime is*

$$N(K) = 2^{2K+1} - 1. \tag{12}$$

Proof. When $K = 0$ there is a unique pair $(1, 1)$, so

$$N(0) = 1. \tag{13}$$

Consider all pairs of nonzero polynomials $f(x)$, $g(x)$ with degree $\leqq k$. Let g.c.d.$(f(x), g(x)) = e(x)$ of degree exactly $L \geqq 0$. Given $e(x)$ there are $N(K-L)$ such pairs. Therefore

$$(2^{K+1}-1)^2 = \sum_{L=0}^{K} 2^L N(K-L). \tag{14}$$

The solution of (13) and (14) is (12). Q.E.D.

COROLLARY 8. *If $m = 2n$ there are 2^{2n-1} values of s for which $M(h, s)$ (or $M_0(h, s)$) has the $2 \times n$ horizontal window property.*

Of course this number is considerably reduced if we require that all possible window properties hold. Table 2 shows the values of s which work for various m and $h(x)$. In the table if s is unstarred then $M(h, s)$ solves Problem (I) and $M_0(h, s)$ solves Problem (II). If s is starred then $M_0(h, s)$ solves Problem (II) but g.c.d.$(s, 2^m - 1) > 1$ and so $M(h, s)$ does not solve Problem (I). The table also gives $N_{\mathrm{I}}(h)$, the total number of s for which $M(h, s)$ solves Problem (I), and $N_{\mathrm{II}}(h)$, the total number of s for which $M_0(h, s)$ solves Problem (II). Rather surprisingly these numbers depend on the choice of $h(x)$. For example when $m = 8$

$$N_{\mathrm{I}}(x^8+x^7+x^6+x^5+x^2+x+1) = 38,$$
$$N_{\mathrm{II}}(x^8+x^7+x^6+x^5+x^2+x+1) = 66,$$

whereas

$$N_{\mathrm{I}}(x^8+x^6+x^5+x+1) = 26,$$
$$N_{\mathrm{II}}(x^8+x^6+x^5+x+1) = 60.$$

3. A shift register which generates the array $M_0(h, s)$. From now on we assume that the array $M_0(h, s)$ has the $m \times 1$ horizontal window property (see Cor. 2). By definition each row of $M_0(h, s)$ is generated by an m-stage linear feedback shift register. In this section we show that successive *columns* of $M_0(h, s)$ are also generated by a shift register.

THEOREM 9. *If $M_0(h, s)$ has the $m \times 1$ horizontal window property then there is an $m \times m$ $(0, 1)$-matrix T such that the columns $\mathbf{c}_0, \mathbf{c}_1, \cdots, \mathbf{c}_{2^m-2}$ of $M_0(h, s)$ are related by*

$$\mathbf{c}_{t+1} = T\mathbf{c}_t, \qquad t = 0, 1, \cdots. \tag{15}$$

Proof. If $M_0(h, s)$ has the $m \times 1$ horizontal window property then by Theorem 1

$$1, \alpha^{-s}, \alpha^{-2s}, \cdots, \alpha^{-(m-1)s}$$

are linearly independent. Hence for any r there is a vector $\mathbf{b}(r) = (b_0, \cdots, b_{m-1})$ such that

$$\alpha^r = \sum_{i=0}^{m-1} b_i \alpha^{-si}.$$

Taking $r = 1$ we find

$$\alpha^{t+1} = \sum_{i=0}^{m-1} b_i \alpha^{t-si},$$

i.e.

$$a_{t+1} = \sum_{i=0}^{m-1} b_i a_{t-si}.$$

Applying this to $r = 1-s, 1-2s, \cdots$ we find that the vectors $\mathbf{b}(1), \mathbf{b}(1-s), \cdots$ are the rows of a matrix T such that (15) holds. Q.E.D.

T can be written down directly from $M_0(h, s)$: the ith column of T is the column of the array that follows the column having a single 1 in the ith place. For example

$M_0(x^6+x+1, 8)$ is shown in Fig. 3, and

$$T = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}. \tag{16}$$

The following properties of T are easily proved: (a) $h(T)=0$ (e.g. (16) satisfies $T^6+T+I=0$), (b) $T^{2^m-1}=I$, and (c)

$$T^s = \begin{bmatrix} b_{m-1} & b_{m-1} & \cdots & b_1 & b_0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

where $x^m+b_{m-1}x^{m-1}+\cdots+b_0$ is the minimal polynomial of α^s.

The matrix T determines an m-stage shift register which generates all the columns of $M_0(h, s)$ from the first column. This is best described by means of an example: Fig. 5 shows the shift register corresponding to (16). The feedback connections contain mod 2 adders $\rightarrow\oplus\rightarrow$ in exactly the locations where T contains 1's. The shift register is shown in a state corresponding to the first column of Fig. 3. Then the next state is the second column, and so on.

Remarks. (i) There are obvious generalizations of this theory to arrays over larger alphabets and to arrays of higher dimension, but we do not pursue these topics here.

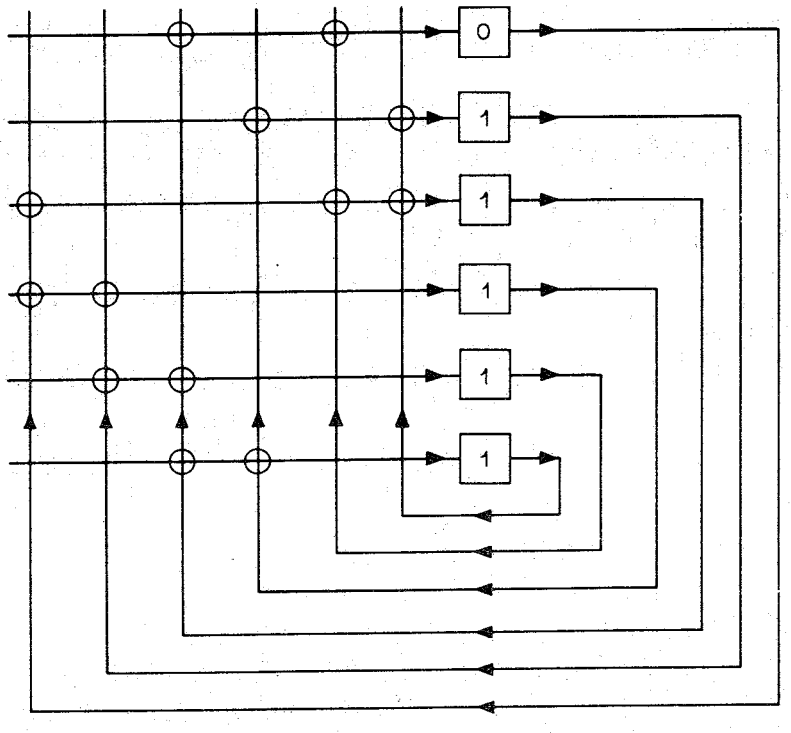

FIG. 5. *The shift register corresponding to the matrix T of Eq.* (16), *which generates successive columns of Fig.* 2.

(ii) One may also study the window properties with the condition that every view, *including the zero view*, appears exactly once. In this case it is trivial to use De Bruijn sequences, [32]–[34], to construct $m \times 2^m$ arrays which have the $m \times 1$ and $1 \times m$ horizontal window properties (including the zero view). For example, if $m = 3$,

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

However, when m is composite it is not in general possible to construct such arrays having all possible window properties. The first example would be a 4×16 array with the 4×1, 2×2 and 1×4 horizontal window properties (including the zero view). But M. E. Best has shown by computer that no such array exists.

REFERENCES

[1] D. CALABRO AND J. K. WOLF, *On the synthesis of two-dimensional arrays with desirable correlation properties*, Information and Control, 11 (1968), pp. 537–560.

[2] A. C. DAVIES AND Y. K. MOY, *Pseudorandom arrays generated by two-dimensional digital filtering*, IEEE Trans. Acoustics, Speech and Signal Processing, ASSP-24 (1976), pp. 332–334.

[3] H. FREDRICKSEN, *On perfect maps*, unpublished.

[4] H. M. FREDRICKSEN, E. C. POSNER AND J. TOWBER, *Perfect maps of special type*, Jet Propulsion Lab, Space Programs Summary, 37-16 (1962), pp. 61–62.

[5] S. W. GOLOMB, ED., *Digital Communications with Space Applications*, Prentice-Hall, Englewood Cliffs, NJ, 1964.

[6] S. W. GOLOMB, *Shift Register Sequences*, Holden-Day, San Francisco, 1967.

[7] B. GORDON, *On the existence of perfect maps*, IEEE Trans. Information Theory, IT-12 (1966), pp. 486–487.

[8] T. IKAI AND Y. KOJIMA, *Two-dimensional cyclic codes*, Electron. Commun. Japan, 57A, no. 4 (1974), pp. 27–35.

[9] T. IKAI, H. KOSAKO AND Y. KOJIMA, *Basic theory of two-dimensional cyclic codes—periods of ideals and fundamental theorems*, Ibid., 59A, no. 3 (1976), pp. 31–38.

[10] ———, *Basic theory of two-dimensional cyclic codes—Structure of cyclic codes and their dual codes*, Ibid., 59A, no. 3 (1976), pp. 39–47.

[11] ———, *Basic theory of two-dimensional cyclic codes—Generator polynomials and the positions of check symbols*, Ibid., 59A, no. 4 (1976), pp. 33–41.

[12] H. IMAI, *Two-dimensional Fire codes*, IEEE Trans. Information Theory, IT-19 (1973), pp. 796–806.

[13] F. J. MACWILLIAMS AND N. J. A. SLOANE, *Pseudo-random sequences and arrays*, Proc. IEEE, 64 (1976), pp. 1715–1729.

[14] T. NOMURA AND A. FUKUDA, *Linear recurring planes and two-dimensional cyclic codes*, Electron. Commun. Japan, 54A, no. 3 (1971), pp. 23–30.

[15] T. NOMURA, H. MIYAKAWA, H. IMAI AND A. FUKUDA, *A method of construction and some properties of planes having maximum area matrix*, Ibid., 54A, no. 4 (1971), pp. 18–25.

[16] ———, *Some properties of the $\gamma\beta$-plane and its extension to three-dimensional space*, Ibid., 54A, no. 8 (1971), pp. 27–34.

[17] ———, *A theory of two-dimensional linear recurring arrays*, IEEE Trans. Information Theory, IT-18 (1972), pp. 775–785.

[18] I. S. REED AND R. M. STEWART, *Note on the existence of perfect maps*, Ibid., IT-8 (1962), pp. 10–12.

[19] R. SPANN, *A two-dimensional correlation property of pseudo-random maximal-length sequences*, Proc. IEEE, 53 (1963), p. 2137.

[20] E. R. BERLEKAMP, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.

[21] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[22] R. W. MARSH, *Table of Irreducible Polynomials over GF(2) through Degree* 19, United States Dept. of Commerce, Washington, DC, 1957.

[23] J. D. SWIFT, *Construction of Galois fields of characteristic two and irreducible polynomials*, Math. Comput., 14 (1960), pp. 99–103.

[24] E. J. WATSON, *Primitive polynomials (mod 2)*, Ibid., 16 (1962), pp. 368–369.
[25] J. D. ALANEN AND D. E. KNUTH, *Tables of finite fields*, Sankhyā, Ser. A. 26 (1964), pp. 305–328.
[26] N. ZIERLER AND J. BRILLHART, *On primitive trinomials (mod 2)*, Information and Control, 13 (1968), pp. 541–554 and 14 (1969), pp. 566–569.
[27] S. MOSSIGE, *Table of Irreducible Polynomials over GF[2] of Degrees 10 through 20*, Dept. of Math., Univ. of Bergen, Bergen, Norway, 2 volumes, 1971.
[28] ———, *Table of irreducible polynomials over GF[2] of degrees 10 through 20*, Math. Comput., 26 (1972), pp. 1007–1009.
[29] W. W. PETERSON AND E. J. WELDON, JR., *Error-Correcting Codes*, M.I.T. Press, Cambridge, MA, 2nd edition, 1972.
[30] W. STAHNKE, *Primitive binary polynomials*, Math. Comput., 27 (1973), pp. 977–980.
[31] D. H. GREEN AND I. S. TAYLOR, *Irreducible polynomials over composite Galois fields and their applications in coding techniques*, Proc. IEE, 121 (1974), pp. 935–939.
[32] N. G. DE BRUIJN, *A combinatorial problem*, Nederl. Akad. Wetensch, Ser. A., 49 (1946), pp. 758–765 = Indag. Math., 8 (1946), 461–467.
[33] H. FREDRICKSEN, *The lexicographically least De Bruijn cycle*, J. Combinatorial Theory, 9 (1970), pp. 1–5.
[34] ———, *A class of nonlinear De Bruijn cycles*, Ibid., 19A (1975), pp. 192–199.