SIAM J. ALG. DISC. METH.
Vol. 1, No. 1, March 1980

0196-5212/80/0101-0014 $01.00/0

ON CONSTRUCTION OF MATRICES WITH DISTINCT SUBMATRICES*

SHARAD V. KANETKAR† AND MEGHANAD D. WAGH‡

Abstract. Given N, M, t and s, a method of generating an $N \times M$ binary matrix such that every nonzero $t \times s$ binary pattern occurs exactly once as its submatrix is presented. This construction is based upon a systematic filling of the matrix with a maximal length recurrent sequence and gives several new solutions yet unreported.

1. Introduction. In this paper we consider the problem of construction of an $N \times M$ binary matrix A such that any $t \times s$ nonzero binary pattern occurs exactly once as its submatrix. Similar problems have been attempted earlier by various authors.

Reed and Stewart [5] considered the existence of A given only t and s. Gordon [2] later extended their result and showed that given any t and s, one can always find N and M, $N > t$, $M > s$ such that all $t \times s$ submatrices (in the toroidal sense) in A are distinct. A is then called a perfect map. All the $t \times s$ nonzero binary patterns are not necessarily the submatrices of a perfect map. However, a perfect map with parameters $M = 2^s - 1$ and $N = (2^{st} - 1)/M$ and containing *all* the $t \times s$ nonzero binary patterns was exhibited in [2]. When N and M are relatively prime, a pseudorandom array also gives a perfect map with the same parameters [3].

The toroidal perfect maps of [2], [3] and [5] can be easily converted into nontoroidal ones by repeating the first $t-1$ rows after the last row and the first $s-1$ columns after the last column. In this paper, we will be concerned only with $N \times M$ nontoroidal perfect map A in which every nonzero binary $t \times s$ pattern occurs exactly once as a submatrix. Obviously, the four parameters are then related as

$$(M-s+1)(N-t+1) = 2^{st} - 1. \tag{1.1}$$

Banerji [1] has recently described a procedure of designing A when (i) $M = s$ and (ii) $M = 2^s + s - 2$. Note that the required matrix A when $M = 2^s + s - 2$ was also obtained earlier by Gordon [2].

In this paper, we give a criterion for filling up the matrix A with a maximal length recurrent sequence (MLRS) such that A will have the required property. Four schemes have been described which satisfy the criterion and hence generate A for all the earlier known cases and for several new ones. This criterion also enables one to construct A for any M, N, s and t satisfying (1.1). We have included here the solution to the problem (for all the possible parameter combinations with $st \leqq 15$) obtained by a computer search made easy with the help of the criterion.

2. Preliminaries. A linear recurrent sequence $\{x_i\}$ of the elements of $GF(q)$, (q: a prime power) of period $q^n - 1$ may be obtained from the recurrence relation

$$x_i = a_1 x_{i-1} + a_2 x_{i-2} + \cdots + a_n x_{i-n} \tag{2.1}$$

over $GF(q)$ with arbitrary nonzero initial condition if the constants $a_1, a_2, \cdots, a_n \in GF(q)$ are chosen such that the polynomial

$$x^n - a_1 x^{n-1} - a_2 x^{n-2} - \cdots - a_n \tag{2.2}$$

is primitive over $GF(q)$. We will use the following property of this maximal length recurrent sequence (MLRS).

---

* Received by the editors November 13, 1978, and in revised form July 13, 1979.

† Computer Centre, Indian Institute of Technology, Bombay 400 076, India.

‡ Department of Electrical Engineering, Indian Institute of Technology, Bombay 400 076, India. Now at Department of Electrical Engineering, Concordia University, 1455 de Maisonneuve Blvd. West, Montreal H3G 1M8, Canada.

LEMMA 1. *Let β be the root of the polynomial* (2.2) *and $i_1, i_2, \cdots, i_n$, any n integers such that $\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_n}$ are linearly independent over $GF(q)$. Then the n-tuple $(x_{i+i_1}, x_{i+i_2}, \cdots, x_{i+i_n})$ assumes all the nonzero values exactly once in the range $0 \leqq i \leqq q^n - 2$.*

Proof. Solution of (2.1) can be expressed as [6]

$$x_i = \mathrm{Tr}\,(b\beta^i),$$

where Tr denotes the trace function

$$\mathrm{Tr}\,(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}$$

from $GF(q^n)$ onto $GF(q)$ and $b \in GF(q^n)$ is determined by the initial conditions. Then

$$\begin{bmatrix} x_{i+i_1} \\ x_{i+i_2} \\ \vdots \\ x_{i+i_n} \end{bmatrix} = \begin{bmatrix} \beta^{i_1} & \beta^{i_1 q} \cdots \beta^{i_1 q^{n-1}} \\ \beta^{i_2} & \beta^{i_2 q} \cdots \beta^{i_2 q^{n-1}} \\ \beta^{i_n} & \beta^{i_n q} \cdots \beta^{i_n q^{n-1}} \end{bmatrix} \begin{bmatrix} b\beta^i \\ (b\beta^i)^q \\ (b\beta^i)^{q^{n-1}} \end{bmatrix}.$$

The matrix on the right-hand side is nonsingular over $GF(q)$ as the elements in the first column are linearly independent by assumption. Thus there is a one-one correspondence between the n-tuple $(x_{i+i_1}, x_{i+i_2}, \cdots, x_{i+i_n})$ and the quantity $b\beta^i$. But as β is the primitive element of $GF(q^n)$, $b\beta^i$ and hence $(x_{i+i_1}, x_{i+i_2}, \cdots, x_{i+i_n})$ takes all the possible $q^n - 1$ nonzero values as i runs over $0 \leqq i \leqq q^n - 2$.

Since we are interested in binary matrices we will restrict ourselves to $q = 2$. However it should be mentioned that the methods developed in this paper can be generalized to the case of matrices with q symbols.

Consider an MLRS $\{x_i\}$ of period $2^{st} - 1$ generated by (2.1) with $n = st$. We now state the central result of this paper.

THEOREM 1. *If A is filled as*

$$A(u, v) = x_{f(u,v)}, \qquad 0 \leqq u \leqq N-1, \quad 0 \leqq v \leqq M-1,$$

such that

(C1) *f is linear in u and v;*

(C2) *when u and v are restricted to $0 \leqq u \leqq N-t$, $0 \leqq v \leqq M-s$, $f(u, v)$ are all distinct modulo $2^{st} - 1$;*

(C3) *$\beta^{f(u,v)}$, $0 \leqq u \leqq t-1$, $0 \leqq v \leqq s-1$ are all linearly independent over $GF(2)$ where β is the root of* (2.2) *with $n = st$;*

then each binary $t \times s$ pattern occurs as a submatrix of A exactly once.

Proof. Denoting $f(u, v)$, $0 \leqq u \leqq t-1$, $0 \leqq v \leqq s-1$ by $i_1, i_2, \cdots, i_{st}$, it is obvious from (C1) that any $t \times s$ submatrix in A with its left-hand top corner at (u, v) has elements

$$x_{i+i_1}, x_{i+i_2}, \cdots, x_{i+i_{st}} \quad \text{where } i = f(u, v).$$

Further, as u, v run over $0 \leqq u \leqq N-t$ and $0 \leqq v \leqq M-s$, (i.e., all possible coordinate values taken by the left hand top corners of $t \times s$ submatrices), i runs over 0 to $2^{st} - 2$ because of (C2) and (1.1). Finally, from (C3), $\beta^{i_1}, \beta^{i_2}, \cdots, \beta^{i_{st}}$ are linearly independent over GF(2) and hence an application of Lemma 1 gives the required result.

3. Generation of A matrix. Several schemes to fill up A to satisfy the conditions (C1)–(C3) may be given.

Scheme 1.

$$f(u, v) = u + tv, \qquad 0 \leqq u \leqq 2^{st} + t - 3, \quad 0 \leqq v \leqq s - 1$$

generates a matrix A with $N = 2^{st} + t - 2$ and $M = s$. Here, (C1) is obvious. To check (C2), note that for $0 \leqq u \leqq N - t$, $0 \leqq v \leqq M - s = 0$, $f(u, v) = u$ and therefore in this range all $f(u, v)$ are distinct modulo $2^{st} - 1$. Finally, the set $\{\beta^{f(u,v)} | 0 \leqq u \leqq t-1, 0 \leqq v \leqq s-1\}$ is $\{1, \beta, \beta^2, \cdots, \beta^{st-1}\}$ elements of which are necessarily linearly independent over $GF(2)$ giving (C3). The generated matrix A will then have the desired properties by Theorem 1. This leads to Banerji's case (i).

The mappings

$$f(u, v) = (M - s + 1)u + v \qquad (H \text{ mapping})$$

$$f(u, v) = u + (N - t + 1)v \qquad (V \text{ mapping})$$

$$0 \leqq u \leqq N - 1, \quad 0 \leqq v \leqq M - 1,$$

obviously satisfy (C1). In the case of H mapping, when u and v are restricted to $0 \leqq u \leqq N - t$, $0 \leqq v \leqq M - s$, one gets $0 \leqq f(u, v) \leqq 2^{st} - 2$ by using (1.1). Thus, if in this range $f(u_1, v_1) \equiv f(u_2, v_2) \pmod{2^{st} - 1}$, then $(M - s + 1)(u_1 - u_2) = (v_2 - v_1)$. But, $M - s + 1$ cannot divide $v_2 - v_1$ (as $0 \leqq v_1, v_2 \leqq M - s$) unless $v_2 = v_1$ and in that case u_1 also equals u_2. Thus $f(u, v)$ are distinct modulo $2^{st} - 1$ in this range showing that (C2) is satisfied. Similarly, V mapping also can be shown to satisfy (C2).

We now present three more schemes based on H and V mappings which satisfy (C3).

Scheme 2. When $t = 1$, choosing H mapping, the set $\{\beta^{f(u,v)} | 0 \leqq u \leqq t - 1 = 0, 0 \leqq v \leqq s - 1\}$ is $\{1, \beta, \beta^2, \cdots, \beta^{s-1}\}$. Its elements are linearly independent over $GF(2)$ as β is the primitive element of $GF(2^{st})$. Thus (C3) is satisfied and the matrix generated will have the required properties.

Scheme 3. When $M = 2s - 1$, using H mapping, $f(u, v) = su + v$. Then the set $\{\beta^{f(u,v)} | 0 \leqq u \leqq t - 1, 0 \leqq v \leqq s - 1\} = \{1, \beta, \beta^2, \cdots, \beta^{st-1}\}$ has elements which are linearly independent over $GF(2)$ as β is the primitive element of $GF(2^{st})$. Thus (C3) is satisfied and one gets the matrix with the required properties.

Scheme 4. Let $z = (2^{st} - 1)/(2^s - 1)$ and j any integer satisfying $j | (2^s - 1)$ and

$$\frac{2^s - 1}{j} \nmid (2^d - 1), \qquad 0 < d < s. \tag{3.1}$$

When A has dimensions $N = zj + t - 1$ and $M = (2^s - 1)/j + s - 1$, one may use V mapping. Then $f(u, v) = u + zjv$. To check (C3) one should prove the linear independence over $GF(2)$ of the elements of $\{\beta^{u+zjv} | 0 \leqq u \leqq t - 1, 0 \leqq v \leqq s - 1\}$. Note that $\beta^z \in GF(2^s)$ and (3.1) implies that β^{zj} does not belong to any subfield of $GF(2^s)$. In other words, $1, \beta^{zj}, \beta^{2zj}, \cdots, \beta^{(s+1)zj}$ are linearly independent over $GF(2)$ because otherwise β^{zj} will satisfy a polynomial of degree $\leqq s - 1$ over $GF(2)$ implying β^{zj} belongs to a proper subfield of $GF(2^s)$. Further, $1, \beta, \beta^2, \cdots, \beta^{t-1}$ are also linearly independent over $GF(2^s)$ because β cannot satisfy a polynomial of degree less than t over $GF(2^s)$. Now if a linear combination of β^{u+zjv} is equal to zero, then

$$\begin{aligned} 0 &= \sum_{u=0}^{t-1} \sum_{v=0}^{s-1} a_{uv} \beta^{u+zjv} \\ &= \sum_{u=0}^{t-1} \left(\beta^u \sum_{v=0}^{s-1} a_{uv} \beta^{zjv} \right), \qquad a_{uv} \in GF(2). \end{aligned}$$

The result of the inner summation belongs to $GF(2^s)$. But as $\{\beta^u | 0 \leqq u \leqq t-1\}$ are linearly independent over $GF(2^s)$, one has from this

$$0 = \sum_{u=0}^{s-1} a_{uv}\beta^{zjv}$$

which, from the linear independence of $\{\beta^{zjv} | 0 \leqq v \leqq s-1\}$ over $GF(2)$ gives $a_{uv} = 0, 0 \leqq u \leqq t-1, 0 \leqq v \leqq s-1$. Thus (C3) is satisfied and A will have the required property.

$j = 1$ trivially satisfies (3.1) and gives dimensions identical to Banerji's case (ii). Table 1 lists the possible values of j for $1 \leqq s \leqq 18$ satisfying (3.1). Each j gives a matrix with distinct parameters.

Example. To illustrate Scheme 4, consider $t = 2$ and $s = 4$. One then has $z = 17$ and by choosing $j = 3$, $N = 52$ and $M = 8$. The required 52×8 binary matrix A may be obtained by

$$A(u, v) = x_{u+51v}, \qquad 0 \leqq u \leqq 51, \quad 0 \leqq v \leqq 7,$$

where $\{x_i\}$ is obtained from the recurrence relation over $GF(2)$:

$$x_i = x_{i-1} + x_{i-2} + x_{i-7} + x_{i-8}$$

(For a list of primitive polynomials over $GF(2)$, refer to [4]). With the initial conditions $x_0 = x_1 = \cdots = x_6 = 0$, $x_7 = 1$, one gets the MLRS as

$$0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ \cdots$$

TABLE 1
Allowed values of j for $1 \leqq s \leqq 18$

s	allowed j
1	1
2	1
3	1
4	1, 3
5	1
6	1, 3, 7
7	1
8	1, 3, 5, 15
9	1, 7
10	1, 3, 11, 31, 93
11	1
12	1, 3, 5, 7, 9, 13, 15, 21, 35, 39, 45, 63, 91, 105, 117, 315
13	1
14	1, 3, 43, 127, 381
15	1, 7, 31, 151, 217
16	1, 3, 5, 15, 17, 51, 85, 255
17	1
18	1, 3, 7, 9, 19, 21, 27, 57, 63, 73, 133, 171, 189, 219, 399, 511, 657, 1197, 1387, 1533, 1971, 4599, 9709, 13797

We give below the transpose of the required matrix whose rows, for convenience, have been coded in right justified octal representation.

0	0	0	6	6	5	0	4	5	7	1	3	0	4	3	1	4	3
1	4	1	4	0	7	3	0	2	5	4	4	7	1	6	5	3	7
1	7	3	3	1	7	0	6	5	6	2	0	7	5	6	7	5	0
0	1	0	0	5	5	7	4	6	7	0	5	6	4	6	2	5	2
0	2	2	1	2	0	4	6	4	3	7	2	6	4	5	1	7	6
0	0	0	6	6	5	0	4	5	7	1	3	0	4	3	1	4	3
1	4	1	4	0	7	3	0	2	5	4	4	7	1	6	5	3	7
1	7	3	3	1	7	0	6	5	6	2	0	7	5	6	7	5	0

4. Solutions for $ts \leqq 15$. The schemes described in the last section do not provide matrix A for all possible combinations of the four parameters satisfying (1.1). However in the cases not covered under the schemes, it may still be possible to obtain the required A matrix by utilizing the V or H mappings described earlier (which already satisfy (C1) and (C2) and finding a primitive polynomial of degree st such that (C3) is also satisfied. This calls for only a checking of linear independence over $GF(2)$ of st different powers of β. With the tables of primitive polynomials already available [4], this task can be performed very rapidly with the help of a computer.

We have made a computer search based on this and have obtained solutions in all the cases for $ts \leqq 15$. The results given in Table 2 provide ready design data in these cases. In this table the entries in the column 'mapping' denote either H mapping or V mapping described in § 3. $N-t+1$ takes all values dividing $2^{st}-1$. M can be computed using (1.1). The primitive polynomials used are:

$$
\begin{aligned}
P1 &: x^6+x+1,\\
P2 &: x^8+x^5+x^3+x+1,\\
P3 &: x^{10}+x^3+1,\\
P4 &: x^{10}+x^4+x^3+x+1,\\
P5 &: x^{12}+x^6+x^4+x+1,\\
P6 &: x^{12}+x^{11}+x^9+x^8+x^7+x^5+x^2+x+1,\\
P7 &: x^{12}+x^{11}+x^{10}+x^8+x^6+x^4+x^3+x+1,\\
P8 &: x^{12}+x^{11}+x^6+x^4+x^2+x+1,\\
P9 &: x^{12}+x^{11}+x^9+x^7+x^6+x^5+1,\\
P10 &: x^{14}+x^{13}+x^{11}+x^7+x^6+x^5+x^4+x^3+x^2+x+1,\\
P11 &: x^{15}+x^{12}+x^9+x^8+x^6+x^3+1,\\
P12 &: x^{15}+x^{14}+x^{12}+x^9+x^8+x^6+x^4+x^3+x^2+x+1.
\end{aligned}
$$

In the cases under Schemes 3 or 4, any primitive polynomial of degree st may be used. The cases when either $N-t+1=1$ (or $M-s+1=1$) or $t=1$ (or $s=1$) are not included in the table as they can be directly obtained from Schemes 1 and 2 respectively.

TABLE 2
Design of A matrix when $ts \leqq 15$

t	s	$N-t+1$	Mapping	Polynomial
2	2	3	H	Any (Scheme 4)
		5	V	Any (Scheme 4)
2	3	3	H	Any (Scheme 4)
		7	H	P1
		9	V	Any (Scheme 4)
		21	H	Any (Scheme 3)
2	4	3	H	Any (Scheme 4)
		5	H	P2
		15	H	P2
		17	V	Any (Scheme 4)
		51	V	Any (Scheme 4)
3	3	7	H	Any (Scheme 4)
		73	V	Any (Scheme 4)
2	5	3	H	Any (Scheme 4)
		11	V	P3
		31	H	P3
		33	V	Any (Scheme 4)
		93	H	P4
2	6	3	H	Any (Scheme 4)
		5	V	P6
		7	H	P8
		9	H	P7
		13	H	P8
		15	H	P9
		21	H	P7
		35	H	P8
		39	H	P8
		45	H	P6
		63	H	P9
		85	V	Any (Scheme 4)
		91	H	P8
		105	H	P8
		117	H	P7
		195	V	Any (Scheme 4)
		273	H	P8
		315	H	P9
		455	V	Any (Scheme 4)
		585	H	P8
3	4	3	V	Any (Scheme 3)
		5	V	P5
		7	H	Any (Scheme 4)
		9	V	P5
		13	V	P5
		15	V	P6
		21	V	P5
		35	V	P6
		39	H	P6
		45	V	P7
		63	H	P7

TABLE 2 (*Contd.*)

t	s	$N-t+1$	Mapping	Polynomial
		85	V	P5
		91	H	P8
		105	V	P5
		117	H	P5
		195	V	P5
		273	V	Any (Scheme 4)
		315	V	P9
		455	V	P5
		585	H	P5
		819	V	Any (Scheme 4)
2	7	3	H	Any (Scheme 4)
		43	H	P10
		127	H	P10
		129	V	Any (Scheme 4)
		381	H	P10
3	5	7	H	Any (Scheme 4)
		31	H	P11
		151	V	P11
		217	V	P11
		1057	V	Any (Scheme 4)
		4081	H	P12

REFERENCES

[1] R. B. BANERJI, *The construction of binary matrices with distinct submatrices*, IEEE Trans. Computers, C-27 (1978), pp. 162–164.

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

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

[4] W. W. PETERSON AND E. J. WELDON, JR, *Error Correcting Codes*, MIT Press, Cambridge, MA, 1972.

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

[6] J. H. VAN LINT, *Coding Theory*, Springer-Verlag, Berlin, 1971.

[7] J. H. VAN LINT, F. J. MACWILLIAMS AND N. J. A. SLOANE, *On pseudo-random arrays*, SIAM J. Appl. Math., 36 (1979), pp. 62–72.