MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 134
APRIL 1976, PAGES 306–311

Characteristic m-Sequences

By Michael Willett

Abstract. The initial k-tuple of the characteristic m-sequence associated with a primitive polynomial of degree k over $GF(2)$ is given for $2 \leqslant k \leqslant 168$.

Introduction. In this note we take advantage of the list of primitive polynomials over $GF(2)$ published by Stahnke [1] to calculate a table of characteristic m-sequences. This author [2] has shown how a characteristic m-sequence may be used to generate a set of cycle representatives for any cyclic code with square-free parity check polynomial. Such cycle sets are important for determining the error-correcting capability of the cyclic code. In [2] cycle set members are formed by adding certain decimations of a characteristic m-sequence. This technique is computationally simpler than standard algorithms based on more complicated algebraic operations.

Preliminaries. Let F be the binary field with two elements 0, 1. A polynomial $f(x) = x^k - a_1x^{k-1} - \cdots - a_k \in F[x]$ is called primitive if a root of $f(x)$ in the extension field $K = GF(2^k)$ of F generates the cyclic multiplicative group of K. There are $\varphi(2^k - 1)/k$ primitive polynomials of degree k, where φ is Euler's function. Assume that $f(x)$ is primitive and consider the linear recursion associated with $f(x)$ given by

$$u_{n+k} = a_1u_{n+k-1} + \cdots + a_ku_n, \qquad n = 0, 1, 2, \ldots . \tag{1}$$

Primitive polynomials are characterized by the fact that every nonzero solution to (1) over F has minimum period $2^k - 1$. Therefore, all nonzero solutions to (1) are cyclic shifts of one another. Any such solution is called an m-sequence (or PN sequence). There exists a unique m-sequence $u = (u_0, u_1, \ldots)$ so that $u_n = u_{2n}$ for all n, called the characteristic m-sequence associated with $f(x)$.

Algorithm. The algorithm used to find the characteristic m-sequence below is easily adapted to finding such sequences over other prime fields. Treat the symbols u_0, $u_1, \ldots, u_{k-1}$ as unknowns. From recursion (1) formally calculate $u_k, u_{k+1}, \ldots,$ u_{2k-2}, reducing each of these terms to a linear combination of the unknowns. Then solve the system of equations

$$u_n = u_{2n}, \qquad n = 0, 1, \ldots, k-1, \tag{2}$$

for the unknowns. The unique nonzero solution will be the characteristic m-sequence associated with $f(x)$. The following table lists the initial k-tuple of the characteristic

Received July 1, 1974; revised June 9, 1975.
AMS (MOS) subject classifications (1970). Primary 12C05, 12C10; Secondary 94A10.

m-sequence associated with the primitive polynomial shown. Each polynomial is given by showing which powers of x appear in $f(x)$; i.e., $f(x) = x^8 + x^6 + x^5 + x + 1$ is given by 8 6 5 1 0. The notation i^n will mean n consecutive copies of the integer i.

The computations were performed on an IBM 370/165 computer. The sequences were verified by checking each sequence with its associated primitive polynomial in equation (2).

Primitive polynomial	Characteristic m-sequence
2 1 0	01
3 1 0	10^2
4 1 0	$0^3 1$
5 2 0	$10^2 10$
6 1 0	$0^5 1$
7 1 0	10^6
8 6 5 1 0	$0^3 101^2 0$
9 4 0	$10^4 10^3$
10 3 0	$0^7 10^2$
11 2 0	$10^8 10$
12 7 4 3 0	$0^5 10^3 1^2 0$
13 4 3 1 0	$10^8 10^3$
14 12 11 1 0	$0^3 101^3 0^2 1010$
15 1 0	10^{14}
16 5 3 2 0	$0^{11} 1010^2$
17 3 0	$101010^3 10^5 1^2 0$
18 7 0	$0^{11} 10^6$
19 6 5 1 0	$10^{12} 10^5$
20 3 0	$0^{17} 10^2$
21 2 0	$10^{18} 10$
22 1 0	$0^{21} 1$
23 5 0	10^{22}
24 4 3 1 0	$0^{21} 101$
25 3 0	10^{24}
26 8 7 1 0	$0^{19} 10^5 1$
27 8 7 1 0	$10^{18} 10^7$
28 3 0	$0^{25} 10^2$
29 2 0	$10^{26} 10$
30 16 15 1 0	$0^{15} 10^{14}$
31 3 0	10^{30}
32 28 27 1 0	$0^5 10^3 1^2 0^2 10101^5 0^4 10^3 10$
33 13 0	10^{32}
34 15 14 1 0	$0^{19} 10^{13} 1$
35 2 0	$10^{32} 10$
36 11 0	$0^{25} 10^{10}$
37 12 10 2 0	$10^{24} 1010^7 10$

Primitive polynomial					Characteristic *m*-sequence
38	6	5	1	0	$0^{33}10^{3}1$
39	4	0			$10^{34}10^{3}$
40	21	19	2	0	$0^{19}1010^{16}10$
41	3	0			10^{40}
42	23	22	1	0	$0^{19}10^{18}1^{2}01$
43	6	5	1	0	$10^{36}10^{5}$
44	27	26	1	0	$0^{17}10^{16}1^{2}0^{7}1$
45	4	3	1	0	$10^{40}10^{3}$
46	21	20	1	0	$0^{25}10^{19}1$
47	5	0			10^{46}
48	28	27	1	0	$0^{21}10^{19}1^{2}0^{4}1$
49	9	0			10^{48}
50	27	26	1	0	$0^{23}10^{22}1^{2}01$
51	16	15	1	0	$10^{34}10^{15}$
52	3	0			$0^{49}10^{2}$
53	16	15	1	0	$10^{36}10^{15}$
54	37	36	1	0	$0^{17}10^{16}1^{2}0^{15}10^{2}$
55	24	0			$10^{30}10^{23}$
56	22	21	1	0	$0^{35}10^{19}1$
57	7	0			10^{56}
58	19	0			$0^{39}10^{18}$
59	22	21	1	0	$10^{36}10^{21}$
60	1	0			$0^{59}1$
61	16	15	1	0	$10^{44}10^{15}$
62	57	56	1	0	$0^{5}10^{4}1^{2}0^{3}1010^{2}1^{4}010^{3}1^{3}0^{2}10^{2}101^{2}$ $01^{3}01^{2}0^{2}1^{2}010101^{4}0$
63	1	0			10^{62}
64	4	3	1	0	$0^{61}101$
65	18	0			$10^{46}10^{17}$
66	10	9	1	0	$0^{57}10^{7}1$
67	10	9	1	0	$10^{56}10^{9}$
68	9	0			$0^{59}10^{8}$
69	29	27	2	0	$10^{66}10$
70	16	15	1	0	$0^{55}10^{13}1$
71	6	0			$10^{64}10^{5}$
72	53	47	6	0	$0^{19}10^{5}10^{12}10^{11}10^{6}10^{5}10^{5}10^{2}$
73	25	0			10^{72}
74	16	15	1	0	$0^{59}10^{13}1$
75	11	10	1	0	$10^{64}10^{9}$
76	36	35	1	0	$0^{41}10^{33}1$
77	31	30	1	0	$10^{46}10^{29}$

Primitive polynomial					Characteristic m-sequences
78	20	19	1	0	$0^{59}10^{17}1$
79	9	0			10^{78}
80	38	37	1	0	$0^{43}10^{35}1$
81	4	0			$10^{76}10^{3}$
82	38	35	3	0	$0^{47}10^{31}10^{2}$
83	46	45	1	0	$10^{36}10^{36}1^{2}0^{7}$
84	13	0			$0^{71}10^{12}$
85	28	27	1	0	$10^{56}10^{27}$
86	13	12	1	0	$0^{73}10^{11}1$
87	13	0			10^{86}
88	72	71	1	0	$0^{17}10^{15}1^{2}0^{14}1010^{13}1^{4}0^{12}10^{3}101$
89	38	0			$10^{50}10^{37}$
90	19	18	1	0	$0^{71}10^{17}1$
91	84	83	1	0	$10^{6}10^{6}1^{2}0^{5}1010^{4}1^{4}0^{3}10^{3}10^{2}1^{2}0^{2}1^{2}0$
					$1010101^{8}0^{7}10^{6}1^{2}0^{5}1010^{4}$
92	13	12	1	0	$0^{79}10^{11}1$
93	2	0			$10^{90}10$
94	21	0			$0^{73}10^{20}$
95	11	0			10^{94}
96	49	47	2	0	$0^{47}1010^{44}10$
97	6	0			$10^{90}10^{5}$
98	11	0			$0^{87}10^{10}$
99	47	45	2	0	$10^{96}10$
100	37	0			$0^{63}10^{36}$
101	7	6	1	0	$10^{94}10^{5}$
102	77	76	1	0	$0^{25}10^{24}1^{2}0^{23}1010^{22}10$
103	9	0			10^{102}
104	11	10	1	0	$0^{93}10^{9}1$
105	16	0			$10^{88}10^{15}$
106	15	0			$0^{91}10^{14}$
107	65	63	2	0	$10^{104}10$
108	31	0			$0^{77}10^{30}$
109	7	6	1	0	$10^{102}10^{5}$
110	13	12	1	0	$0^{97}10^{11}1$
111	10	0			$10^{100}10^{9}$
112	45	43	2	0	$0^{67}1010^{42}$
113	9	0			10^{112}
114	82	81	1	0	$0^{33}10^{31}1^{2}0^{30}1010^{13}1$
115	15	14	1	0	$10^{100}10^{13}$
116	71	70	1	0	$0^{45}10^{44}1^{2}0^{23}1$
117	20	18	2	0	$10^{96}1010^{15}10$

Primitive polynomial					Characteristic m-sequences
118	33	0			$0^{85}10^{32}$
119	8	0			$10^{110}10^{7}$
120	118	111	7	0	$0^{9}1010101011^{3}01^{3}01^{2}0^{3}1^{2}01^{2}0101^{2}01^{2}$ $01^{3}0^{3}1^{3}0^{2}1010^{2}1^{4}01^{4}0^{2}1^{3}0^{2}1^{4}0^{2}101^{2}$ $0^{2}101^{3}0^{4}10^{2}1^{6}010^{2}1^{2}01^{3}010^{2}$
121	18	0			$10^{102}10^{17}$
122	60	59	1	0	$0^{63}10^{57}1$
123	2	0			$10^{120}10$
124	37	0			$0^{87}10^{36}$
125	108	107	1	0	$10^{16}10^{16}1^{2}0^{15}1010^{14}1^{4}0^{13}10^{3}10^{12}1^{2}$ $0^{2}1^{2}0^{11}101010$
126	37	36	1	0	$0^{89}10^{35}1$
127	1	0			10^{126}
128	29	27	2	0	$0^{99}1010^{26}$
129	5	0			10^{128}
130	3	0			$0^{127}10^{2}$
131	48	47	1	0	$10^{82}10^{47}$
132	29	0			$0^{103}10^{28}$
133	52	51	1	0	$10^{80}10^{51}$
134	57	0			$0^{77}10^{56}$
135	11	0			10^{134}
136	126	125	1	0	$0^{11}10^{9}1^{2}0^{8}1010^{7}1^{4}0^{6}10^{3}10^{5}1^{2}0^{2}1^{2}0^{4}$ $101010100^{3}1^{8}0^{2}10^{7}101^{2}0^{6}1^{3}010^{5}10^{2}1^{3}$ $0^{4}1^{2}010^{3}$
137	21	0			10^{136}
138	8	7	1	0	$0^{131}10^{5}1$
139	8	5	3	0	$10^{130}10^{7}$
140	29	0			$0^{111}10^{28}$
141	32	31	1	0	$10^{108}10^{31}$
142	21	0			$0^{121}10^{20}$
143	21	20	1	0	$10^{122}10^{19}$
144	70	69	1	0	$0^{75}10^{67}1$
145	52	0			$10^{92}10^{51}$
146	60	59	1	0	$0^{87}10^{57}1$
147	38	37	1	0	$10^{108}10^{37}$
148	27	0			$0^{121}10^{26}$
149	110	109	1	0	$10^{38}10^{38}1^{2}0^{37}1010^{29}$
150	53	0			$0^{97}10^{52}$
151	3	0			10^{150}
152	66	65	1	0	$0^{87}10^{63}1$
153	1	0			10^{152}

Primitive polynomial					Characteristic m-sequences
154	129	127	2	0	$0^{25}1010^{22}10^{3}10^{20}10101010^{18}10^{7}10^{16}$ $1010^{5}1010^{14}10^{3}$
155	32	31	1	0	$10^{122}10^{31}$
156	116	115	1	0	$0^{41}10^{39}1^{2}0^{38}1010^{31}1$
157	27	26	1	0	$10^{130}10^{25}$
158	27	26	1	0	$0^{131}10^{25}1$
159	31	0			10^{158}
160	19	18	1	0	$0^{141}10^{17}1$
161	18	0			$10^{142}10^{17}$
162	88	87	1	0	$0^{75}10^{73}1^{2}0^{10}1$
163	60	59	1	0	10^{162}
164	14	13	1	0	$0^{151}10^{11}1$
165	31	30	1	0	$10^{134}10^{29}$
166	39	38	1	0	$0^{127}10^{37}1$
167	6	0			$10^{160}10^{5}$
168	17	15	2	0	$0^{151}1010^{14}$

Department of Mathematics
University of North Carolina
Greensboro, North Carolina 27412

1. W. STAHNKE, "Primitive binary polynomials," *Math. Comp.*, v. 27, 1973, pp. 977–980. MR **48** #6064.

2. M. WILLETT, "Cycle representatives for minimal cyclic codes," *IEEE Trans. Information Theory*, v. 21, 1975, pp. 716–718.