INFORMATION AND CONTROL 39, 149–157 (1978)

On the Toggle Register Polynomial

WAYNE STAHNKE

11434 McCune Avenue, Los Angeles, California 90066

A toggle register is a loop of n binary storage elements, of which t are trigger flip-flops and the remainder are delay flip-flops. If $0 < t < n$, the state structure of a toggle register consists of pure cycles, the length and number of which can be determined from the properties of the toggle register polynomial $x^n + (x + 1)^t$ over the field of two elements. For certain values of n and t the toggle register polynomial is primitive, and a corresponding toggle register generates a binary sequence of period $2^n - 1$ that exhibits randomness properties. In this paper we investigate the properties of the toggle register polynomial. The results can be summarized as follows: $x^n + (x + 1)^t$ is irreducible if and only if $x^n + x^t + 1$ is irreducible and $(n, t) = 1$; $x^n + (x + 1)^t$ is primitive if and only if $x^n + x^t + 1$ is primitive and $(2^n - 1, t) = 1$. The accompanying list gives all irreducible toggle register polynomials and their indices through degree 137.

INTRODUCTION

In attempting to generate binary sequences with desirable properties, particularly binary pseudorandom sequences, several investigators have studied trinomials over the field of two elements. This study was motivated by the fact that a trinomial of degree n corresponds to a logical network that consists of only n delay flip-flops and a single two-input modulo-two adder (Golomb, 1967). However, there is a simpler configuration of logical elements that can generate sequences with desirable properties. This is the toggle register, which is a loop of n binary storage elements, of which t are trigger flip-flops and the remainder are delay flip-flops. The loop may contain an arbitrary number of complementations. A trigger flip-flop is a binary storage element whose next output differs from its present output if its present input is a 1; if its present input is a 0, its output does not change. A type of universal flip-flop known as a "JK flip-flop" can function as either a trigger flip-flop or a delay flip-flop; thus, a toggle register can be constructed from JK flip-flops only.

In their paper on toggle registers, Alltop *et al.* (1968) showed that for $0 < t < n$, the state diagram of a toggle register is partitioned into disjoint cycles whose lengths and number depend only on n and t (Alltop *et al.*, 1968, Theorem 1, p. 194). Thus, for the purpose of studying the state structure, an arbitrary toggle register may be replaced by the related linear toggle register that has the

same arrangement of trigger flip-flops and delay flip-flops, but does not contain any complementations. If this is done, the individual columns of the state cycles all satisfy the difference equation that corresponds to the polynomial $x^{n-t}(x+1)^t + 1$ (Alltop *et al.*, 1968, Theorem 2, p. 195). Therefore, the study of the cycle structure of toggle registers reduces to the study of the properties of $f(x) = x^{n-t}(x+1)^t + 1$ (see Elspas, 1959). The reciprocal polynomial $x^n f(1/x) = x^n + (x+1)^t$ retains all of the properties of the original polynomial, and has the advantage that it is mathematically more tractable. This polynomial is studied here, with t limited to $0 < t < n$ throughout this paper. We call the polynomial $x^n + (x+1)^t$ the *toggle register polynomial.*

The restriction $0 < t < n$ eliminates the cases $t = 0$ and $t = n$. If $t = 0$, the toggle register degenerates into a loop of n delay flip-flops, which has been studied by Golomb (1967, pp. 118–122, 171–175). The state diagram of this configuration consists of disjoint cycles that all have short periods. If the loop contains an even number of complementations, the maximal period is n, and if it contains an odd number of complementations, the maximal period is $2n$. If $t = n$, the toggle register reduces to a loop of n trigger flip-flops, whose state diagram consists of disjoint bushes rather than disjoint cycles. The number and structure of the bushes can be determined by a technique given by Crowell (1962) and Gill (1966).

Preliminary Results

The factorization of $x^n + (x+1)^{n-t}$ can be obtained from the factorization of $x^n + (x+1)^t$ in the following way. The reciprocal polynomial of $x^n + (x+1)^t$ is $x^{n-t}(x+1)^t + 1$, and the reciprocal polynomial of $x^n + (x+1)^{n-t}$ is $x^t(x+1)^{n-t} + 1$. Each one of these reciprocals can be obtained from the other one by substituting $x + 1$ for x, either in the polynomial itself or in its factorization. Since this substitution preserves the degree of each factor, the factorization obtained in this way is complete, although the period of an irreducible derived factor may be different from the period of the irreducible factor that generated it.

This construction effectively reduces the problem of the factorization of $x^n + (x+1)^t$ for $0 < t < n$ to the problem of the same factorization for $0 < t \leqslant n/2$. Since $x^n + (x+1)^t$ and $x^n + (x+1)^{n-t}$ always have the same number of irreducible factors, $x^n + (x+1)^t$ is irreducible if and only if $x^n + (x+1)^{n-t}$ is irreducible.

The factorization of the toggle register polynomial is further simplified by two theorems, the first of which depends on the following lemma:

Lemma 1. *The toggle register polynomial $x^n + (x+1)^t$ does not contain a first-degree factor.*

Proof. Every root of a first-degree factor of $x^n + (x+1)^t$ is also a root of $x^n + (x+t)^t$. The only first-degree polynomials are x and $x+1$, which have the roots 0 and 1, respectively. Neither 0 nor 1 is a root of $f(x) = x^n + (x+1)^t$, since $f(0) = f(1) = 1$.

THEOREM 1. *The toggle register polynomial $x^n + (x+1)^t$ contains a repeated factor if and only if $2 \mid (n, t)$, and in that case $x^n + (x+1)^t$ is a square.*

Proof. The proof is divided into three cases.

Case 1. $n \equiv t \equiv 0 \bmod 2$. In this case, $x^n + (x+1)^t = [x^{n/2} + (x+1)^{t/2}]^2$, and the result follows.

Case 2. $n + t \equiv 1 \bmod 2$. Here any repeated factor of $f(x) = x^n + (x+1)^t$ is also a factor of its formal derivative $f'(x) = nx^{n-1} + t(x+1)^{t-1}$. Since only one of n and t is odd, $f'(x)$ is either a power of x or a power of $x+1$, both of which are relatively prime to $x^n + (x+1)^t$ by Lemma 1. Hence, there cannot be a repeated factor in this case.

Case 3. $n \equiv t \equiv 1 \bmod 2$. Any common factor of $f(x)$ and $f'(x)$ is also a factor of $f(x) + xf'(x) = x^n + (x+1)^t + x[x^{n-1} + (x+1)^{t-1}] = (x+1)^t + x(x+1)^{t-1} = (x+1)^{t-1}$ which is relatively prime to $x^n + (x+1)^t$ by Lemma 1. Hence, there is no repeated factor in this case.

THEOREM 2. *If $(n, t) > 1$, $x^n + (x+1)^t$ is divisible by a toggle register polynomial of lower degree.*

Proof. The assertion follows from $a + b \mid a^k + b^k$ for $k \geqslant 1$, where we take $k = (n, t)$, $a = x^{n/k}$, $b = (x+1)^{t/k}$.

For broad classes of polynomials, the conclusion can hold even if $(n, t) = 1$. To see this, reduce n and t modulo $2^m - 1$. If the resulting polynomial is divisible by an irreducible polynomial of degree m, that polynomial also divides $x^n + (x+1)^t$. A specific example is $x^{19} + (x+1)^{18}$, which is divisible by $x^4 + (x+1)^3$.

THE TOGGLE REGISTER POLYNOMIAL AND ITS CORRESPONDING TRINOMIAL

In this section we show that for $(n, t) = 1$, all of the properties of the toggle register polynomial $x^n + (x+1)^t$ can be derived from the properties of its *corresponding trinomial* $x^n + x^t + 1$.

LEMMA 2. *Let α be a root of $x^n + x^t + 1$. Then α^t is a root of $x^n + (x+1)^t$.*

Proof. Since $\alpha^n + \alpha^t + 1 = 0$, we have $\alpha^n = \alpha^t + 1$. Then by substitution, $(\alpha^t)^n + (\alpha^t + 1)^t = (\alpha^t)^n + (\alpha^n)^t = 0$, and therefore α^t is a root of $x^n + (x+1)^t$.

Lemma 2 provides a means of beginning the factorization of the toggle register polynomial from the factorization of $x^n + x^t + 1$. In general, the factorization obtained in this way is not complete. If $(n, t) = 1$, however, the factorization is complete. Theorem 3 is a statement of this fact.

THEOREM 3. *If* $(n, t) = 1$, *each irreducible factor of degree* m *of* $x^n + (x + 1)^t$ *is the minimal polynomial of the* tth *power of any root of a unique irreducible factor of degree* m *of* $x^n + x^t + 1$.

Proof. Let α be a root of order q of an irreducible factor of degree m of $x^n + x^t + 1$. Then α^t is a root of $x^n + (x + 1)^t$ by Lemma 2, and α^t has order $q/(q, t)$ and degree M, a divisor of m. Since $(n, t) = 1$, we have $M = m$, which can be shown as follows. By the definition of degree, $q/(q, t) \mid 2^M - 1$. Hence $q \mid (q, t)(2^M - 1)$, which implies that $q \mid t(2^M - 1)$. The field element $\alpha^t + 1 = \alpha^n$ also has degree M, so in a similar way we have $q \mid n(2^M - 1)$. Therefore $q \mid (n, t)(2^M - 1)$, which implies that $q \mid 2^M - 1$. This happens if and only if $m \mid M$. The requirements that $m \mid M$ and $M \mid m$ imply that $M = m$. Thus the minimal polynomial of α^t has degree m. Every root of the irreducible factor of $x^n + x^t + 1$ generates the same irreducible factor of $x^n + (x + 1)^t$, since the tth powers of the conjugates of α are the conjugates of α^t.

Two distinct irreducible factors of $x^n + x^t + 1$ cannot generate the same irreducible factor of $x^n + (x + 1)^t$. To see this, let ω^p be a root of an irreducible factor of degree m of $x^n + n^t + 1$, where ω is any primitive element of $GF(2^m)$. If there exists a different irreducible factor of $x^n + x^t + 1$ that generates the same factor of $x^n + (x + 1)^t$, it must be of degree m, as shown above, and therefore it has a root ω^q that satisfies $(\omega^p)^t = (\omega^q)^t$, by Lemma 2. Hence $(\omega^{p-q})^t = 1$. But $(\omega^p)^t = (\omega^q)^t$ if and only if $(\omega^p)^t + 1 = (\omega^q)^t + 1$, which implies that $(\omega^p)^n = (\omega^q)^n$, since ω^p and ω^q are both roots of $x^n + x^i + 1$. Therefore $(\omega^{p-q})^n = 1$. Taking $\alpha = \omega^{p-q}$, we have $\alpha^t = 1 = \alpha^n$. Since the order of α divides both n and t, it must divide $(n, t) = 1$. Therefore the order of α is 1, which implies that $\alpha = \omega^{p-q} = 1$. This is true only if $\omega^p = \omega^q$, which contradicts the hypothesis that the irreducible factors of $x^n + x^t + 1$ are distinct.

The possibility of repeated factors is ruled out by Theorem 1. Thus, the theorem is proved.

COROLLARY 1. *If* $(n, t) = 1$, *the period of* $x^n + (x + 1)^t$ *divides the period of* $x^n + x^t + 1$.

COROLLARY 2. *If* $(n, t) = 1$, $x^n + (x + 1)^t$ *and* $x^n + x^t + 1$ *have the same number of irreducible factors.*

Using Theorem 3, we can obtain the cycle structure of a toggle register polynomial from the factorization of its corresponding trinomial if $(n, t) = 1$ by calculating the period p of each irreducible factor of $x^n + (x + 1)^t$ from the

period q of each irreducible factor of $x^n + x^t + 1$ by $p = q/(q, t)$. Golomb (1967) has given a table of the complete factorization of $x^n + n^t + 1$ for $n \leqslant 36$.

Corollary 2 implies that the result of Swan (1962), that gives the parity of the number of irreducible factors of $x^n + x^t + 1$, also gives the parity of the number of irreducible factors of $x^n + (x + 1)^t$ if $(n, t) = 1$. If we combine Theorem 2 with Swan's corollary 5 (1962, p. 1105) we get the following result.

Let $0 < t \leqslant n/2$ (for $n/2 < t < n$, substitute $n - t$ for t). Then $x^n + (x + 1)^t$ is reducible in the following cases:

(1) $n \equiv 0 \bmod 8$,
(2) $n \equiv \pm 1 \bmod 8$, $t = 2$,
(3) $n \equiv 2 \bmod 8$, $t \not\equiv -1 \bmod 4$,
(4) $n \equiv -2 \bmod 8$, $t \not\equiv 1 \bmod 4$,
(5) $n \equiv \pm 3 \bmod 8$, $t \neq 2$,
(6) $(n, t) > 1$.

In all other cases $x^n + (x + 1)^t$ has an odd number of irreducible factors, all of which are distinct.

Case 1 is interesting because it gives a class of degrees for which no irreducible toggle register polynomials exist. To exhibit other classes of reducible toggle register polynomials, we can apply to Case 5 the fact that an irreducible polynomial of period q that divides $x^n + x^2 + 1$ also divides $x^m + x^2 + 1$ if and only if $m \equiv n \bmod q$. In particular, the toggle register polynomial is reducible if

(1) $n \equiv 13$ or $19 \bmod 24$,
(2) $n \equiv 3, 13, 27$, or $45 \bmod 56$, $n > 3$,
(3) $n \equiv 53, 69, 83$, or $99 \bmod 120$,
(4) $n \equiv \pm 5, 59, \pm 67, \pm 69, \pm 117, 133, 195$, or $245 \bmod 248$, $n > 5$,

and so forth. By Theorem 6, the cases listed above are also cases for which $x^n + x^t + 1$ is imprimitive.

Irreducible Toggle Register Polynomials

We are now in a position to present necessary and sufficient conditions for the irreducibility of the toggle register polynomial.

Theorem 4. *The toggle register polynomial $x^n + (x + 1)^t$ is irreducible if and only if $x^n + x^t + 1$ is irreducible and $(n, t) = 1$.*

Proof. If $x^n + (x + 1)^t$ is irreducible, $(n, t) = 1$ by Theorem 2, and therefore $x^n + x^t + 1$ is irreducible by Corollary 2. On the other hand, if $x^n + x^t + 1$ is irreducible and $(n, t) = 1$, $x^n + (x + 1)^t$ is irreducible by Corollary 2.

In certain cases, the following two theorems simplify the task of finding irreducible toggle register polynomials.

THEOREM 5. *If* $(2^n - 1, n) = 1$, $x^n + (x + 1)^t$ *is irreducible if and only if* $x^n + x^t + 1$ *is irreducible.*

Proof. If $x^n + x^t + 1$ is irreducible, it has a root α in $GF(2^n)$. Let the order of α be q. Then $(q, n) = 1$, since $q \mid 2^n - 1$ and $(2^n - 1, n) = 1$. Thus the order $q/(q, n)$ of α^n is q. Therefore the degree of α^n is n, the degree of α, and the degree of $\alpha^n + 1$ is also n. But $\alpha^t = \alpha^n + 1$, since α is a root of $x^n + x^t + 1$. Thus α^t is a root in $GF(2^n)$ of degree n of $x^n + (x + 1)^t$ by Lemma 2, which implies that $x^n + (x + 1)^t$ is irreducible. On the other hand, if $x^n + x^t + 1$ is reducible, $x^n + (x + 1)^t$ is reducible by Theorem 4.

COROLLARY 3. *If* n *is a prime or a prime power,* $x^n + (x + 1)^t$ *is irreducible if and only if* $x^n + x^t + 1$ *is irreducible.*

Proof. Let $n = p^m$, where p is a prime. Every prime factor of $2^n - 1$ is of the form $kp + 1$, and therefore relatively prime to p. Thus $(2^n - 1, n) = 1$, and the conclusion follows.

LEMMA 3. *If* $k > 1$, $x^{kn} + x^{kt} + 1$ *is imprimitive.*

Proof. If $x^{kn} + x^{kt} + 1$ is primitive, it has a root α in $GF(2^{kn})$ of order $2^{kn} - 1$. By substitution, α^k is a root of $x^n + x^t + 1$.

Since $x^{kn} + x^{kt} + 1$ is primitive, it is irreducible. As a consequence, $x^n + x^t + 1$ is also irreducible, since if $f(x)$ divides $x^n + x^t + 1$, $f(x^k)$ divides $x^{kn} + x^{kt} + 1$. Hence the order $(2^{kn} - 1)/(2^{kn} - 1, k)$ of α^k must divide $2^n - 1$. This implies that $2^{kn} - 1$ divides $k(2^n - 1)$, which is not true for any $k > 1$.

THEOREM 6. *If* $x^n + x^t + 1$ *is primitive,* $x^n + (x + 1)^t$ *is irreducible.*

Proof. If $x^n + x^t + 1$ is primitive it is irreducible, and $(n, t) = 1$ by Lemma 3. Hence, $x^n + (x + 1)^t$ is irreducible by Theorem 4.

PRIMITIVE TOGGLE REGISTER POLYNOMIALS

If the toggle register polynomial is primitive, the state diagram of a corresponding toggle register consists of a long cycle of period $2^n - 1$ and a short cycle of period 1. If in addition the toggle register is taken to be linear (that is, if all complementations are removed from the loop), the sequences that appear at the output of each flip-flop all satisfy the difference equation that corresponds to the reciprocal of the toggle register polynomial $x^n + (x + 1)^t$. Therefore each one of these sequences is just a phase shift of any other one. Thus, dis-

TABLE I

Complete List of n and t for All Irreducible Toggle Register Polynomials $x^n + (x + 1)^t$ through $n = 137$*

n	t	n	t
2	1	63	1, 5, 11(7), 31, 32, 52(7), 58, 62
3	1, 2	65	18, 32, 33, 47
4	1, 3(3)	68	9(3), 33(3), 35(5), 59
5	2, 3	71	6, 9, 18, 20, 35, 36, 51, 53, 62, 65
6	1, 5	73	25, 28, 31, 42, 45, 48
7	1, 3, 4, 6	74	35(3), 39(3)
9	1(7), 4, 5, 8(7)	76	21(3), 55(15)
10	3(3), 7	79	9, 19, 60, 70
11	2, 9	81	4, 16, 35(7), 46, 65, 77(7)
12	5(5), 7(35)	84	5(5), 11(5), 13(13), 71, 73(5), 79(5)
14	5(3), 9(3)	86	21(3), 65(3)
15	1, 4, 7(7), 8, 11, 14(7)	87	13, 74
17	3, 5, 6, 11, 12, 14	89	38, 51
18	7(7), 11	92	21(15), 71(5)
20	3(3), 17	93	2, 91(7)
21	2, 19	94	21(3), 73
22	1, 21(3)	95	11, 17, 78, 84
23	5, 9, 14, 18	97	6, 12, 33, 34, 63, 64, 85, 91
25	3, 7, 18, 22	98	11, 27(3), 71, 87(3)
28	1(15), 3(3), 9(3), 13, 15(15), 19, 25(5), 27(15)	100	19(41), 37, 49(11), 51(33), 63(3), 81(123)
29	2, 27	102	29(3), 37(3), 65(3), 73(3)
30	1(99), 29(99)	103	9, 13, 30, 31, 72, 73, 90, 94
31	3, 6, 7, 13, 18, 24, 25, 28	105	4(49), 8(7), 16, 17, 37, 43, 52, 53, 62(31), 68, 88, 89, 97(7), 101(49)
33	10(7), 13, 20, 23(161)	106	15(3), 91
34	7(3), 27(3)	108	17(5), 31, 77(7), 91(455)
35	2, 33	111	10, 49(7), 62, 101
36	11, 25(5)	113	9, 15, 30, 83, 98, 104
39	4, 8, 14(7), 25, 31, 35(7)	118	33(3), 45(3), 73, 85
41	3, 20, 21, 38	119	8, 38, 81, 111
44	5(15), 39(15)	121	18, 30(23), 91(23), 103
46	1(3), 45(3)	123	2, 121
47	5, 14, 20, 21, 26, 27, 33, 42	124	19(3), 37, 45(15), 55(5), 69(15), 79(5), 87(3), 105(15)
49	9, 12, 15, 22, 27, 34, 37, 40	127	1, 7, 15, 30, 63, 64, 97, 112, 120, 126
52	3(3), 7(3), 19, 21(3), 31, 33(3), 45(15), 49	129	5, 31, 46, 83, 98(7), 124
55	7(23), 24, 31(31), 48(23)	130	3(3), 127
57	4(7), 7(7), 22, 25(7), 32(7), 35(7), 50, 53(7)	132	17(35), 29, 103, 115(805)
58	19, 39(3)	134	57(3), 77
60	1, 11(11), 17(1155), 23(5), 37(5), 43(1155), 49(7), 59	135	11, 16, 22, 29(151), 106(151), 113, 119(7), 124(31)
62	29(3), 33(3)	137	21, 35, 57, 80, 102, 116

* For each imprimitive polynomial, the index is given in parentheses.

regarding the trivial 1-cycle, the output sequence associated with the toggle register is unique. The sequence exhibits randomness and autocorrelation properties that have been studied by Zierler (1959) and Golomb (1967). Lemma 2 implies that the sequence consists of a "decimation by t" of the sequence generated by the reciprocal of the corresponding trinomial; see Selmer (1966).

Theorem 7 gives necessary and sufficient conditions for the primitivity of the toggle register polynomial.

THEOREM 7. *The toggle register polynomial* $x^n + (x+1)^t$ *is primitive if and only if* $x^n + x^t + 1$ *is primitive and* $(2^n - 1, t) = 1$.

Proof. If $x^n + x^t + 1$ is primitive, it has a root α in $GF(2^n)$ of order $2^n - 1$. The order of α^t is also $2^n - 1$, since $(2^n - 1, t) = 1$. But α^t is a root of $x^n + (x+1)^t$, by Lemma 2. It follows that $x^n + (x+1)^t$ is irreducible with period $2^n - 1$, that is, it is primitive.

On the other hand, if $x^n + (x+1)^t$ is primitive it is irreducible. Thus, $x^n + x^t + 1$ is irreducible and $(n, t) = 1$ by Theorem 4. The period of $x^n + x^t + 1$ is a multiple of $2^n - 1$ by Corollary 1, and therefore equal to $2^n - 1$, since the period of an irreducible polynomial of degree n divides $2^n - 1$.

COROLLARY 4. *If* n *is a prime,* $x^n + (x+1)^t$ *is primitive if and only if* $x^n + x^t + 1$ *is primitive.*

Proof. If n is a prime, every prime factor of $2^n - 1$ is of the form $kn + 1$, and therefore relatively prime to t. Thus $(2^n - 1, t) = 1$, and the conclusion follows.

THE ACCOMPANYING LIST

The list that accompanies this paper (Table I) gives all irreducible toggle register polynomials and their indices (index $= (2^n - 1)/\text{period}$) through degree 137. The factorizations of $2^n - 1$ used to generate the list are from Riesel (1968), with one exception. The factorization of $2^{137} - 1$ is from Brillhart *et al.* (1975).

The list can be extended by the use of Zierler and Brillhart (1968, 1969) which gives all irreducible trinomials through degree 1000, and the periods and indices of those for which the factorization of $2^n - 1$ was known at the time the paper was written. Some primitive toggle register polynomials of very high degree can be found in Zierler (1969), which gives a list of all irreducible trinomials for the first 23 values of n for which $2^n - 1$ is prime. Since $2^n - 1$ prime requires n prime, Corollary 4 implies that Zierler's list is a list of primitive toggle register polynomials.

ACKNOWLEDGMENT

The author is indebted to Dr. Raymond Redheffer for his valuable assistance in the preparation of this paper.

RECEIVED: December 16, 1977

REFERENCES

ALLTOP, W. O., PRATT, A. V., AND BURTON, R. C. (1968), Algebraic theory of flip-flop sequence generators, *Inform. Contr.* **12**, 193–205.

BERLEKAMP, E. R. (1968), "Algebraic Coding Theory," McGraw–Hill, New York.

BRILLHART, J., LEHMER, D. H., AND SELFRIDGE, J. L. (1975), New primality criteria and factorizations of $2^m \pm 1$, *Math. Comp.* **29**, 620–647.

CROWELL, R. H. (1962), Graphs of linear transformations over finite fields, *J. Soc. Ind. Appl. Math.* **10**, 103–112.

ELSPAS, B. (1959), The theory of autonomous linear sequential networks, *IRE Trans. Circuit Theory* **CT-6**, 45–60.

GILL, A. (1966), "Linear Sequential Circuits," McGraw–Hill, New York.

GOLOMB, S. W. (1967), "Shift Register Sequences," Holden–Day, San Francisco.

MCELIECE, R. J. (1969), Factorization of polynomials over finite fields, *Math. Comp.* **23**, 861–867.

MYKKELTVEIT, J. (1972), A proof of Golomb's conjecture for the de Bruijn graph, *J. Combinatorial Theory* **13**, 40–45.

PETERSON, W. W. (1961), "Error-Correcting Codes," M.I.T. Press, Cambridge, Mass.

RIESEL, H. (1968), "En Bok om Primtal," Studenttlitteratur, Odense, Denmark.

SELMER, E. S. (1966), "Linear Recurrence Relations over Finite Fields," Department of Mathematics, University of Bergen, Bergen, Norway.

STAHNKE, W. (1973), Primitive binary polynomials, *Math. Comp.* **27**, 977–980.

SWAN, R. G. (1962), Factorization of polynomials over finite fields, *Pacific J. Math.* **12**, 1099–1106.

ZIERLER, N. (1959), Linear recurring sequences, *J. Soc. Ind. Appl. Math.* **7**, 31–48.

ZIERLER, N. (1969), Primitive trinomials whose degree is a Mersenne exponent, *Inform. Contr.* **15**, 67–69.

ZIERLER, N. (1970), On $x^n + x + 1$ over $GF(2)$, *Inform. Contr.* **16**, 502–505.

ZIERLER, N., AND BRILLHART, J. (1968), On primitive trinomials (mod 2), *Inform. Contr.* **13**, 541–554.

ZIERLER, N., AND BRILLHART, J. (1969), On primitive trinomials (mod 2), II, *Inform. Contr.* **14**, 566–569.