By Corollary 12, we know if \( q > 3 \) then there exist \((n - 1)\)th CI functions which are not linear. We now give our main result.

**Theorem 13 (Main Theorem):** Every \((n - 1)\)th CI function with \( n \) variables over \( F_q \) is linear if and only if \( q = 2, 3 \).

**Proof:** The sufficiency is proved by Lemma 2 and Theorem 4 while the necessity is proved by the constructive result of Corollary 12.

### III. Conclusions

We have determined that the only finite fields for which every \((n - 1)\)-CI function is linear are the fields \( F_2 \) and \( F_3 \). Our results may be useful in constructing combinations of generating functions over large fields with both high-order correlation immunity and large linear complexity. Although the \((n - 1)\)-CI nonlinear functions we have constructed have diagonal types, they still give satisfactory linear complexities, especially for large \( q \). If the variable \( x_i \) is fed by a source \( m \)-sequence \( \pi \), which is generated by a primitive polynomial of degree \( l \), then the linear complexity of the function in Corollary 12 is

\[
\sum_{i=0}^{n} \binom{l_i + q - 3}{q - 2}
\]

For linear complexity analysis, see [6].

### ACKNOWLEDGMENT

The authors wish to express their sincere thanks to the referees for their important comments, especially for indicating two up-to-date relevant references ([7], [8]) which were published during the refereeing process of our correspondence. Using results from [7] and [8], one could provide a shorter proof of Theorem 4.

### REFERENCES


### On the Linear Complexity of Legendre Sequences

Cunsheng Ding, Tor Helleseth, Fellow, IEEE, and Weijuan Shan

**Abstract**—In this correspondence we determine the linear complexity of all Legendre sequences and the (monic) feedback polynomial of the shortest linear feedback shift register that generates such a Legendre sequence. The result of this correspondence shows that Legendre sequences are quite good from the linear complexity viewpoint.

**Index Terms**—Codes, cryptography, Legendre sequence, sequence.

### I. INTRODUCTION

Let \( p \) be a prime. The Legendre sequence \( s^n \) with respect to the prime \( p \) is defined by

\[
s_i = \begin{cases} 
1 + \left( \frac{i}{p} \right) & \text{if } i \neq 0 \mod p \\
0 & \text{otherwise}
\end{cases}
\]

for each \( i \geq 0 \), where \((i/p)\) is the Legendre symbol. Here and hereafter Legendre sequences are viewed as binary sequences over the finite field \( \text{GF}(2) \).

Legendre sequences have a number of interesting properties, we refer to [1]–[4] for details. In this correspondence we determine the linear complexity of all Legendre sequences and the (monic) feedback polynomial of the shortest linear feedback shift register (for short, LFSR) that generates such a Legendre sequence. The result of this correspondence shows that Legendre sequences are quite good from the linear complexity viewpoint.

### II. LINEAR COMPLEXITY

Let \( s^n = s_0, s_1, \ldots, s_{n-1} \) be a sequence over a field \( F \). The linear complexity or linear span of \( s^n \) is defined to be the shortest positive integer \( l \) such that there are constants \( c_0 = 1, c_1, \ldots, c_l \in F \) satisfying

\[
s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdots + c_l s_{i-l}, \quad \text{for all } l \leq i < n.
\]

Such a polynomial \( r(x) = c_0 + c_1 x + \cdots + c_l x^l \) is called the feedback polynomial of a shortest linear feedback shift register (LFSR) that generates \( s^n \). Hereafter we use feedback polynomial for short. Such an integer always exists for finite sequences \( s^n \). When \( n = \infty \), a sequence \( s^\infty \) is called a semi-infinite sequence. If there is no such integer for a semi-infinite sequence \( s^\infty \), its linear complexity is defined to be \( \infty \). For ultimately periodic semi-infinite sequences such an \( l \) always exists. The linear complexity of periodic sequences can be expressed simply as follows.

Let \( s^m \) be a sequence of period \( n \) over a field \( F \), and

\[
S^n(x) = s_0 + s_1 x + \cdots + s_{n-1} x^{n-1}.
\]

Manuscript received August 10, 1996; revised October 23, 1997.

C. Ding is with the Department of Information Systems and Computer Science, The National University of Singapore, Singapore 119260 (e-mail: dingcs@ics.nus.edu.sg).

T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: tor.helleseth@ii.uib.no).

W. Shan is with Department of Applied Mathematics, Xidian University, Xian 710071, China.

Publisher Item Identifier S 0018-9448(98)02364-5.
Then it is easy to see that [7]

1) the feedback polynomial of $s^\infty$ is given by

$$x^n - 1 / \gcd(x^n - 1, S^\infty(x)),$$

(1)

2) the linear complexity of $s^\infty$ is given by

$$n - \deg(\gcd(x^n - 1, S^n(x))).$$

(2)

One of our two main results is stated in the following theorem.

**Theorem 1:** Let $s^\infty$ be the Legendre sequence of period $p$ as before. Then

1) if $p = 8t - 1$ for some $t$, then $L(s^\infty) = (p + 1)/2$;
2) if $p = 8t + 1$ for some $t$, then $L(s^\infty) = (p - 1)/2$;
3) if $p = 8t + 3$ for some $t$, then $L(s^\infty) = p$; and
4) if $p = 8t + 5$ for some $t$, then $L(s^\infty) = p - 1$.

**Proof:** For simplicity we use $L_p$ to denote the linear complexity of the Legendre sequence with period $p$. Let $Q$ denote the set of quadratic residues $q$ with $0 < q \leq p - 1$ and $N$ the set of quadratic nonresidues modulo $p$. Define

$$S^\infty(x) = \sum_{q \in Q} x^q,$$

and let $\beta$ be a primitive $\rho$th root of unity over the field $GF(2^n)$ that is the splitting field of $x^p - 1$. Then by (2) we have

$$L_p = \deg\left[\left(x^p - 1\right)/\gcd(x^p - 1, S^\infty(x))\right] = p - \left|\left\{j : S^\infty(\beta^j) = 0, \ 0 \leq j \leq p - 1\right\}\right|.$$  

(3)

Before calculating the actual linear complexity, we have to mention the following basic facts:

**B1:** $(Q, \cdot)$ is a group with $|Q| = (p - 1)/2$ and $q \cdot N = N$ for any $q \in Q$, where $\cdot$ denotes integer multiplication modulo $p$.

**B2:** $S^\infty(\beta^n) = S^\infty(\beta)$ for any $q \in Q$ and $S^\infty(\beta^n) = 1 + S^\infty(\beta)$ for any $n \in N$.

**B3:** $S^\infty(\beta) \in \{0, 1\}$ if and only if $2 \in Q$.

**B4:** $2 \in Q$ if and only if $p = 8t \pm 1$ for some $t$ [5].

Basic fact B1 is straightforward.

Since $(Q, \cdot)$ is a group, we have $qQ = Q$ and $q^{-1} \in Q$ for any $q \in Q$. Hence,

$$S^\infty(\beta^n) = \sum_{q \in Q} \beta^{q^2} = \sum_{q \in Q} \beta^q = S^\infty(\beta).$$

Since $n^{-1} \in N$ for any $n \in N$ and $nQ = N$, we have

$$S^\infty(\beta^n) = \sum_{q \in Q} \beta^{q^n} = \sum_{n \in N} \beta^n = 1 + S^\infty(\beta)$$

which completes the proof of B2.

Since the characteristic of the field $GF(2^n)$ is 2, it follows that $(S^\infty(\beta))^2 = S^\infty(\beta^n)$, and therefore B3 follows from B2 by observing that $(S^\infty(\beta))^2 = S^\infty(\beta)$ if and only if $2 \in Q$.

The proof of B4, based on the Law of Quadratic Reciprocity, can be found in [5].

Thus we have completed the proofs of the above basic facts that will be used frequently in the sequel.

The proof of Theorem 1 is then completed by considering two cases depending on whether $2$ is a quadratic residue or nonresidue.

We first consider the case $2 \in Q$, which according to B4 happens if and only if $p = 1$ or $7$ mod $8$. It follows from B3 that $S^\infty(\beta) \in \{0, 1\}$ and from B2 that either $S^\infty(\beta^n) = 0$ for all $q \in Q$ or $S^\infty(\beta^n) = 0$ for all $n \in N$. Since $S^\infty(1) = [p - 1]/2$ mod $4$, it follows that $S^\infty(1) = 0$ if $p = 1$ mod $16$ and $S^\infty(1) = \neq 0$ if $p = 7$ mod $8$. Hence if $p = 1$ mod $8$ then by (3)

$$L_p = p - \left|\left\{j : S^n(\beta^j) = 0, \ 0 \leq j \leq p - 1\right\}\right| = p - (p - 1)/2 - 1 = (p - 1)/2$$

and if $p = 7$ mod $8$ then by (3)

$$L_p = p - (p - 1)/2 - (p + 1)/2.$$  

Finally, we consider the case $2 \not\in Q$, which according to B4 happens if and only if $p = 3$ or $5$ mod $8$. From B3 it follows that $S^\infty(\beta) \not\in \{0, 1\}$. Since $-1 = 1$, B2 implies that $S^\infty(\beta^n) = 0$ for all $j$ with $0 < j \leq p - 1$. Since $S^\infty(1) = [p - 1]/2$ mod $2$, it follows that $S(1) = 1$ if $p = 3$ mod $8$ and $S^\infty(1) = 0$ if $p = 5$ mod $8$. Thus if $p = 3$ mod $8$ then by (3)

$$L_p = p - \left|\left\{j : S^n(\beta^j) = 0, \ 0 \leq j \leq p - 1\right\}\right| = p$$

and if $p = 5$ mod $8$ then by (3)

$$L_p = p - \left|\left\{j : S^n(\beta^j) = 0, \ 0 \leq j \leq p - 1\right\}\right| = p - 1.$$  

Hence, we have completed the proof of Theorem 1.

**Remark:** Parts 1 and 3 of this theorem are implied in [6].

III. FEEDBACK POLYNOMIAL

In the preceding section we have calculated the linear complexity of Legendre sequences with a simple approach. In this section we determine the feedback polynomials of Legendre sequences.

In the case that $2 \in Q$, let $\beta$ be a primitive $\rho$th root over $GF(2^n)$ as before. Since $S^\infty(\beta^2) = S^\infty(\beta)$, we have $S^\infty(\beta) = 0$ or 1. By B2, $S^\infty(\beta^2) = 1 + S^\infty(\beta)$ for any $n \in N$. So, replacing $\beta$ by $\beta^n$, if necessary, we can choose the primitive root $\beta$ to have the property that $S^\infty(\beta) = 1$. Since $2 \in Q$, we have $Q = 2Q$ and $N = 2N$.

Hence,

$$q(x) = \prod_{\gamma \in Q}(x - \beta^{\gamma}) \quad \text{and} \quad n(x) = \prod_{n \in N}(x - \beta^n)$$

have coefficients from $GF(2)$. The polynomials $q(x)$ and $n(x)$ depend on the choice of $\beta$, but there are only two possibilities. In the sequel, we shall fix the $\beta$ as above, i.e., $S^\infty(\beta) = 1$.

**Theorem 2:** Let $s^\infty$ be the Legendre sequence of period $p$ as before and $m(x)$ its feedback polynomial. Then

1) if $p = 8t - 1$ for some $t$, then $m(x) = (x - 1)q(x)$;
2) if $p = 8t + 1$ for some $t$, then $m(x) = q(x)$;
3) if $p = 8t + 3$ for some $t$, then $m(x) = x^n - 1$; and
4) if $p = 8t + 5$ for some $t$, then $m(x) = (x^n - 1)/(x - 1)$.

**Proof:** Recall the proof of Theorem 1, in the previous section. We first consider the case 2 $\in Q$. Then the polynomials $q(x)$ and $n(x)$ have coefficients from $GF(2)$, and

$$x^n - 1 = (x - 1)q(x)n(x).$$

Recall that $2 \in Q$ is equivalent to $p = 1$ or $7$ mod $8$. In the case that $p = 7$ mod $8$, the proof of Theorem 1 has shown that $S^\infty(1) = 1$. From our choice of $\beta$ and the proof of Theorem 1 it follows that $S^\infty(\beta^n) = S(\beta) = 1 \neq 0$ for all $q \in Q$ and, therefore, $S^\infty(\beta^n) = 0$ for all $n \in N$. We obtain that

$$\gcd(x^n - 1, S^\infty(x)) = n(x).$$

Hence, by (1) we have

$$m(x) = \frac{x^n - 1}{\gcd(x^n - 1, S^\infty(x))} = (x - 1)q(x).$$

Similarly, if $p = 1$ mod $8$, the proof of Theorem 1 has shown that $S^\infty(1) = 0$ and from our choice of $\beta$ we get $S^\infty(\beta^n) = 1$ for all $q \in Q$ and $S^\infty(\beta^n) = 0$ for all $n \in N$. It follows that

$$\gcd(x^n - 1, S^\infty(x)) = (x - 1)n(x).$$
Hence, by (1) we have
\[ m(x) = \frac{x^n - 1}{\gcd(x^n - 1, S^p(x))} = q(x). \]

Now we consider the case \( 2 \not\in Q \). The proof of Theorem 1 has shown that in this case
\[ S^p(\beta^j) \neq 0, \quad \text{for } 0 < j \leq p - 1. \]

Further, \( S^p(1) = 1 \) if \( p = 3 \mod 8 \) and \( S^p(1) = 0 \) if \( p = 5 \mod 8 \).
It follows that
\[ \gcd(x^n - 1, S^p(x)) = \begin{cases} 1, & \text{if } p = 3 \mod 8 \\ x - 1, & \text{if } p = 5 \mod 8. \end{cases} \]

Hence, by (1)
\[ m(x) = \frac{x^n - 1}{\gcd(x^n - 1, S^p(x))} = \begin{cases} x^n - 1, & \text{if } p = 3 \mod 8 \\ x - 1, & \text{if } p = 5 \mod 8. \end{cases} \]

Hence, we have completed the proof of Theorem 2.

ACKNOWLEDGMENT

The authors wish to thank the referees for their comments and suggestions that improved the correspondence, and for pointing out [6].

REFERENCES


Binary Pseudorandom Sequences of Period \( 2^n - 1 \) with Ideal Autocorrelation Generated by the Polynomial \( z^d + (z + 1)^d \)

Jong-Seon No, Habong Chung, and Min-Seon Yun

Abstract—In this correspondence, we present a construction for binary pseudorandom sequences of period \( 2^n - 1 \) with ideal autocorrelation property using the polynomial \( z^d + (z + 1)^d \). We show that the sequence obtained from the polynomial becomes an \( m \)-sequence for certain values of \( d \). We also find a few values of \( d \) which yield new binary sequences with ideal autocorrelation property when \( m \) is \( 3k \pm 1 \), where \( k \) is a positive integer. These new sequences are represented using trace function and the results are tabulated.

Index Terms—Binary sequences, ideal autocorrelation, polynomial, pseudorandom sequences.

I. INTRODUCTION

A binary \( (0 \text{ or } 1) \) sequence \( \{a(t), t = 0, 1, \ldots, N - 1\} \) of period \( N = 2^n - 1 \) is said to have the ideal autocorrelation property if its periodic autocorrelation function \( R_a(\tau) \) is given by
\[ R_a(\tau) = \begin{cases} N, & \text{for } \tau \equiv 0 \mod N \\ -1, & \text{for } \tau \not\equiv 0 \mod N \end{cases} \]

where \( R_a(\tau) \) is defined as
\[ R_a(\tau) = \sum_{t=0}^{N-1} (-1)^{(t+\tau)+a(t)} \]

and \( \tau + \tau \) is computed modulo \( N \).

Some of the well-known binary sequences of period \( 2^n - 1 \) include \( m \)-sequences, GMW sequences, generalized GMW sequences, “Legendre” sequences, Hall’s sextic residue sequences, extended sequences, and miscellaneous sequences of which the construction methods are not known yet. These sequences are best described in terms of the trace function over a finite field. Let \( GF(2^m) \) be the finite field with \( 2^m \) elements. Let \( m = en > 1 \) for some positive integers \( e \) and \( n \). Then the trace function \( tr_{2^e}^n(\cdot) \) is a mapping from \( GF(2^m) \) to its subfield \( GF(2^n) \) given by [2]
\[ tr_{2^e}^n(x) = \sum_{i=0}^{n-1} x^{2^{ei}}. \]

In this correspondence, we present a construction for binary pseudorandom sequences of period \( 2^n - 1 \) with ideal autocorrelation property using the polynomial \( z^d + (z + 1)^d \). These sequences are found by a computer search. In Section II, we show that \( m \)-sequences can be obtained by this method for certain values of \( d \). In Section III, we also find a few values of \( d \) which yield new binary sequences with ideal autocorrelation property when \( m \) is \( 3k \pm 1 \), where \( k \) is a positive integer. These new sequences are represented using trace function and the results are tabulated.

Manuscript received September 24, 1997; revised November 29, 1997. This work was supported by the Institute of Information Technology Assessment under Grants 96003-RT-11 and 96190-CT-12 from the Korean Ministry of Information and Communications. J.-S. No and M.-S. Yun are with the Department of Electronic Engineering, Konkuk University, Seoul 143-701, Korea. H. Chung is with the School of Electronic and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea.

Publisher Item Identifier S 0018-9448/98/02365-7.