Bull. Korean Math. Soc. 29 (1992), No. 1, pp. 89–99

THE PERIOD AND THE LINEAR COMPLEXITY OF CERTAIN LINEAR RECURRING SEQUENCES IN THE FINITE FIELD $GF(q)$

SEUNG AHN PARK

1. Introduction

Let $GF(q)$ be a finite field with q elements, where q is a prime power. A sequence

$$s_0, s_1, s_2, \cdots, s_t, s_{t+1}, \cdots$$

of elements of $GF(q)$ is denoted by $\{s_t\}$. The set $GF(q)^\omega$ of all sequences in $GF(q)$ forms an algebra over $GF(q)$ under the addition, multiplication and the scalar multiplication defined as follows:

$$\begin{aligned} \{u_t\} + \{v_t\} &= \{u_t + v_t\}, \\ \{u_t\}\{v_t\} &= \{u_t v_t\}, \\ c\{u_t\} &= \{cu_t\} \end{aligned}$$

If there exists a positive integer r such that $s_{t+r} = s_t$ for all $t \geq 0$, then $\{s_t\}$ is said to be *periodic*, and the smallest positive integer r such that $s_{t+r} = s_t$ for all $t \geq 0$ is called the *period* of the sequence.

Let $c_0, c_1, \cdots, c_{n-1}$ be given elements of the finite field $GF(q)$. A sequence $\{s_t\}$ in $GF(q)$ satisfying the linear recurrence relation

$$s_{t+n} = \sum_{i=1}^{n-1} c_i s_{t+i} \qquad (t = 0, 1, 2, \cdots)$$

is called an n-th *homogeneous linear recurring sequence* in $GF(q)$ and the polynomial

$$f(x) = -c_0 - c_1 x - c_2 x^2 - \cdots - c_{n-1} x^{n-1} + x^n$$

Received March 23, 1991.
This reaserch has been supported by Korea Research Foundation.

is called the *characteristic polynomial* of $\{s_t\}$. And for any monic polynomial

$$g(x) = -a_0 - a_1 x - a_2 x^2 - \cdots - a_{n-1} x^{n-1} + x^n$$

over $GF(q)$ of degree $n \geq 1$, a sequence $\{s_t\}$ in $GF(q)$ satisfying

$$s_{t+n} = \sum_{i=0}^{n-1} a_i s_{t+i} \qquad (t = 0, 1, 2, \cdots)$$

is said to be *generated* by $g(x)$. The set of all homogeneous linear recurring sequence in $GF(q)$, generated by $g(x)$ forms a subspace of the vector space $GF(q)^\omega$, which is called the *solution space* of $g(x)$ and is denoted by $S(g(x))$.

Let $\{s_t\}$ be a homogeneous linear recurring sequence in $GF(q)$. Then there exists a unique monic polynomial $h(x) \in GF(q)[x]$, $\deg h(x) \geq 1$, such that for any monic polynomal $g(x) \in GF(q)[x]$ we have

$$\{s_t\} \in S(g(x)) \quad \text{if and only if} \quad h(x) | g(x).$$

The polynomal $h(x)$ is called the *minimum polynomial* of $\{s_t\}$ and the degree of $h(x)$ is called the *linear complexity* or *linear equivalence* of $\{s_t\}$.

In this paper we will prove some theorems on the period and the linear complexity of certain sequences in $GF(q)$ which are generated by combining two sequences in a reasonable way. In fact these theorems are generalizations of the main result in [1].

A sequence of elements of $GF(2)$ is called a binary sequence. In recent years considerable interest has been shown in the generation of binary sequences which have good properties. Such binary sequences play an important role in a stream cipher system.

The terminology and the notation in this paper are standard, and they are taken from [3]. Throughout this paper, $GF(q)$ denotes the finite field with q elements, where q is a prime power.

2. Preliminaries

In this section we will state some propositions which are useful in proving theorems in section 3. The proofs of these propositions will be omitted and they can be found in [3] and [6].

Let $GF(q)$ be the finite field with q elements, where q is a prime power, and let $f(x) \in GF(q)[x]$ be a polynomial of degree $n \geq 1$ with $f(0) \neq 0$. Then there exits a positive integer $e \leq q^n - 1$ such that $f(x) | (x^e - 1)$ in $GF(q)[x]$. The smallest positive integer e such that $f(x) | (x^e - 1)$ in $GF(q)[x]$ is called the *order* of $f(x)$ and is denoted by $\operatorname{ord} f(x)$. If $f(x)$ is an irreducible polynomial over $GF(q)$ of degree n, then the order of $f(x)$ divides $q^n - 1$.

The multiplicative group $GF(q)^* = GF(q) - \{0\}$ is cyclic. A generator of the cyclic group $GF(q)^*$ is called a *primitive element* of $GF(q)$. A polynomial $f(x) \in GF(q)[x]$ of degree $n \geq 1$ is called a *primitive polynomial* if it is the minimum polynomial over $GF(q)$ of a primitive element of $GF(q^n)$. A monic polynomial $f(x) \in GF(q)[x]$ of degree n is a primitive polynomial over $GF(q)$ if and only if it is irreducible over $GF(q)$ and $\operatorname{ord} f(x) = q^n - 1$.

Let $\{s_t\}$ be any sequence in $GF(q)$ and let d be a positive integer. A sequence $\{u_t\}$ such that

$$u_t = s_{t+d} \qquad (t = 0, 1, 2, \cdots)$$

is called the *translate* of $\{s_t\}$ by d, and it is denoted by ${}_d\{s_t\}$. And a sequence $\{v_t\}$ such that

$$v_t = s_{dt} \qquad (t = 0, 1, 2, \cdots)$$

is called the *decimation* of $\{s_t\}$ by d, and it is denoted by $\{s_t\}^{(d)}$.

PROPOSITION 2.1. *Let $\{s_t\}$ be a homogeneous linear recurring sequence genereted by a polynomial $f(x) \in GF(q)[x]$ of degree $n \geq 1$. Then the period of the sequence divides* $\operatorname{ord} f(x)$ *and so it is $\leq q^n - 1$.*

If $h(x) \in GF(q)[x]$ is the minimum polynomial of $\{s_t\}$, then the period of the sequence is equal to $\operatorname{ord} h(x)$.

PROPOSITION 2.2. *Let $f(x)$ be a primitive polynomial over $GF(q)$ of degree $n \geq 1$. Then any nonzero sequence in $GF(q)$ generated by $f(x)$ is of period $q^n - 1$.*

Such a sequence is called a *maximal period sequence* in $GF(q)$.

PROPOSITION 2.3. *Let $f(x) \in GF(q)$ be a primitive polynomial of degree $n \geq 1$ and let $\{s_t\}$ be a nonzero sequence generated by $f(x)$. Then the sequence $\{s_t\}$ in $GF(q)$ is a maximal period sequence of period $q^n - 1$ and*

$$S(f(x)) = \left\{ {}_i\{s_t\} \mid 0 \leq i \leq q^n - 2 \right\} \cup \{\{0\}\}.$$

PROPOSITION 2.4. *Let $f(x) \in GF(q)[x]$ be an irreducible polynomial of degree $n \geq 1$ such that $\alpha \in GF(q^n)$ is a root of $f(x)$, and let d be a positive integer. If $h(x)$ is an irreducible polynomial over $GF(q)$ of degree n with $h(\alpha^d) = 0$, then*

$$S(h(x)) = \left\{ \{s_t\}^{(d)} \mid \{s_t\} \in S(f(x)) \right\}.$$

PROPOSITION 2.5. *Let*

$$f_1(x),\ f_2(x),\ \cdots,\ f_r(x)$$

be all the distinct monic irreducible polynomials in $GF(q)[x]$ of degree n and order N, and let $M \geq 2$ be an integer which satisfies the following two conditions:

(i) *All prime factors of M divide N but not $(q^n - 1)/N$.*
(ii) *$q^n \equiv 1 \pmod 4$ if $M \equiv 0 \pmod 4$.*

Then

$$f_1(x^M),\ f_2(x^M),\ \cdots,\ f_r(x^M)$$

are all the distinct monic irreducible polynomials in $GF(q)[x]$ of degree nM and order NM.

3. The period and the linear complexity of certain sequences

Let $GF(q)$ be the finite field with q elements, where q is a prime power. In this section we will study the period and the linear complexity of certain sequences which are generated by combining two maximal period sequences in $GF(q)$.

Let $f(x)$ and $g(x)$ be primitive polynomials over $GF(q)$ of degree m and n respectively, where $m > 1$ and $n > 1$. Let k be an integer such that

$$1 \leq k < m$$

and let $i_1, i_2, \cdots, i_{k-1}$ be integers such that

$$0 < i_1 < i_2 < \cdots < i_{k-1} < m.$$

And let $\mathbf{Z}_q = \{0, 1, 2, \cdots, q-1\}$ be the set of all nonnegative integers less than q, and let

$$\tau : GF(q) \longrightarrow \mathbf{Z}_q,\ \tau(a) = a'$$

be any injective map such that $\tau(0) = 0$.

Let $\{a_t\}$ and $\{b_t\}$ be nonzero sequences in $GF(q)$ generated by $f(x)$ and $g(x)$, respectively. Thus $\{a_t\}$ and $\{b_t\}$ are maximal period sequences of period $q^m - 1$ and $q^n - 1$, respectively. For each vector

$$(a_t, a_{t+i_1}, \cdots, a_{t+i_{k-1}}) \in GF(q)^k \qquad (t = 0, 1, 2, \cdots)$$

let R_t be an integer given by

$$R_t = a'_t q^{k-1} + a'_{t+i_1} q^{k-2} + \cdots + a'_{t+i_{k-1}} \qquad (t = 0, 1, 2, \cdots)$$

and let $\{u_t\}$ be a sequence in $GF(q)$ such that

$$u_t = b_{d_t} \qquad (t = 0, 1, 2, \cdots)$$

where

$$d_t = t + \sum_{i=0}^{t} R_i \qquad (t = 0, 1, 2, \cdots)$$

From now on we will study the period and the linear complexity of the sequence $\{u_t\}$ in $GF(q)$. The notation introduced in the above sentences will keep its meaning throughout this section.

THEOREM 3.1. *Let*

$$M = q^m - 1, \quad N = q^n - 1, \quad K = M + \sum_{t=0}^{M-1} R_t.$$

Then the following hold.

(1) $K = M + \dfrac{q^m(q^k-1)}{2} = \dfrac{q^m(q^k+1)}{2} - 1$

(2) $({}_i\{u_t\})^{(M)} = ({}_{d_i}\{b_t\})^{(K)} \qquad (i = 0, 1, \cdots, M-1)$

Proof. (1) Since $\{a_t\}$ is a maximal period sequence of period M, we have

$$\{(a_t, a_{t+1}, \cdots, a_{t+m-1}) \mid 0 \le t \le M-1\} \cup \{(0, \cdots, 0)\} = GF(q)^m$$

by Proposition 2.3. Hence

$$\{(a_t, a_{t+i_i}, \cdots, a_{t+i_{k-1}}) \mid 0 \le t \le M-1\} = GF(q)^k$$

and every nonzero vector in $GF(q)^k$ occurs exactly q^{m-k} times while t varies from 0 to $M-1$. Since

$$\tau : GF(q) \longrightarrow \mathbf{Z}_q. \ \tau(a) = a'$$

is injective map such that $\tau(0) = 0$, it follows that

$$\{(a'_t, a'_{t+i_1}, \cdots, a'_{t+i_{k-1}}) \mid 0 \le t \le M-1\} = \mathbf{Z}_{q^k}$$

and every nonzero vector in $\mathbf{Z}_{q^k}$ occurs exactly q^{m-k} times while t varies from 0 to $M-1$. Therefore, we have

$$\begin{aligned}\sum_{t=0}^{M-1} R_t &= \sum_{t=0}^{M-1} a'_t q^{k-1} + a'_{t+i_1} q^{k-2} + \cdots a'_{t+i_{k-1}} \\ &= q^{m-k}\{1 + 2 + \cdots + (q^k - 1)\} = \frac{q^m(q^k-1)}{2}\end{aligned}$$

and

$$K = M + \sum_{t=0}^{M-1} R_t = q^m - 1 + \frac{q^m(q^k-1)}{2} = \frac{q^m(q^k+1)}{2} - 1$$

(2) Since $\{a_t\}$ is a periodic sequence of period M, we have

$$R_{i+jM} = R_i \qquad (0 \le i \le M-1,\ \ j = 0, 1, 2, \cdots)$$

and so

$$\begin{aligned} d_{i+jM} &= i + jM + \sum_{t=0}^{i+jM} R_t = jM + j\sum_{t=0}^{M-1} R_t + i + \sum_{t=0}^{i} R_t \\ &= jK + d_i \qquad (0 \le i \le M-1,\ \ j = 0, 1, 2, \cdots) \end{aligned}$$

Therefore, we have

$$u_{i+jM} = b_{jK+d_i} \qquad (0 \le i \le M-1,\ j = 0, 1, 2, \cdots)$$

and so $({}_i\{u_t\})^{(M)} = ({}_{d_i}\{b_t\})^{(K)} \quad (i = 0, 1, \cdots, M-1)$.

THEOREM 3.2. *Let*

$$M = q^m - 1,\ \ N = q^n - 1,\ \ K = M + \frac{q^m(q^k-1)}{2}$$

Let β be a primitive element of $GF(q^n)$ such that $g(\beta) = 0$ and let $h(x)$ be the minimum polynomial of β^K over $GF(q)$.

If $(N, K) = 1$, then the following hold.

(1) *The polynomial $h(x)$ is a primitive polynomial over $GF(q)$ such that $\deg h(x) = n$, $\operatorname{ord} h(x) = N$, and $h(x) = \prod_{i=0}^{n-1}(x - \beta^{Kq^i})$.*

(2) *For each $j = 0, 1, 2, \cdots$, the sequence $({}_j\{b_t\})^{(K)}$ in $GF(q)$ has $h(x)$ as its miminum polynomial and it is of period N.*

(3) *The sequence $\{u_t\}$ in $GF(q)$ is generated by the polynomial $h(x^M)$ over $GF(q)$, and*

$$h(x^M) = \prod_{i=0}^{n-1}(x^M - \beta^{Kq^i}), \qquad \deg h(x^M) = nM.$$

Proof. By assumption $g(x)$ is a primitive polynomial over $GF(q)$ of degree n, and so there exists a primitive element $\beta \in GF(q^n)$ such that $g(\beta) = 0$.

(1) We have $GF(q^n)^* = \langle \beta \rangle$ and $|GF(q^n)^*| = q^n - 1 = N$. Since $(N, K) = 1$ it follows that $GF(q^n)^* = \langle \beta^K \rangle$. Therefore, β^K is a primitive element of $GF(q^n)$ and the order of $h(x)$ is N. Hence the assertion (1) holds.

(2) Since $g(x)$ is a primitive polynomial over $GF(q)$ with $g(\beta) = 0$ and $\{b_t\}$ is a nonzero sequence generated by $g(x)$, we have

$$S(g(x)) = \{{}_j\{b_t\} \mid 0 \le j \le N-1\} \cup \{\{0\}\}$$

by Proposition 2.3. Hence we have

$$S(h(x)) = \{({}_j\{b_t\})^{(K)} \mid 0 \le j \le N-1\} \cup \{\{0\}\}$$

by Proposition 2.4. Therefore, each sequence $({}_j\{b_t\})^{(K)}$ has $h(x)$ as its miminum polynomial and it is of period N.

Thus the assertion (2) holds.

(3) Arrange elements of $\{u_t\}$ as follows :

$$\begin{array}{llll} u_0 & u_M & u_{2M} & \cdots \\ u_1 & u_{M+1} & u_{2M+1} & \cdots \\ \vdots & \vdots & \vdots & \\ u_{M-1} & u_{M+M-1} & u_{2M+M-1} & \cdots \end{array}$$

In this way we obtain M sequences

$$\{u_t\}^{(M)},\ ({}_1\{u_t\})^{(M)},\ \cdots,\ ({}_{M-1}\{u_t\})^{(M)}$$

in $GF(q)$. On the other hand, we have

$$({}_i\{u_t\})^{(M)} = ({}_{d_i}\{b_t\})^{(K)} \qquad (i = 0, 1, \cdots, M-1)$$

by Theorem 3.1. Hence each $({}_i\{u_t\})^{(M)}$ has $h(x)$ as its minimum polynomial and $({}_i\{u_t\})^{(M)} \in S(h(x))$ by the assertion (2).

Suppose that

$$h(x) = -c_0 - c_1 x - \cdots - c_{n-1}x^{n-1} + x^n \in GF(q)[x].$$

Then, for each $i = 0, 1, \cdots, M-1$, we have

$$u_{M(t+n)+i} = \sum_{j=0}^{n-1} c_j u_{M(t+j)+i}, \qquad (t = 0, 1, 2, \cdots)$$

In particular we have

$$u_{t+nM} = \sum_{j=0}^{n-1} c_j u_{t+jM}, \qquad (t = 0, 1, 2, \cdots)$$

and so $\{u_t\}$ is generated by the polynomial

$$h(x^M) = -c_0 - c_1 x^M - \cdots - c_{n-1}x^{(n-1)M} + x^{nM} \in GF(q)[x].$$

Hence the assertion (3) holds.

THEOREM 3.3. *Assume that the following three conditions hold.*

(i) $\left(q^n - 1,\ q^m - 1 + \frac{q^m(q^k-1)}{2}\right) = 1.$

(ii) $q^n \equiv 1 \pmod 4$ *if* $q^m \equiv 1 \pmod 4$

(iii) *All prime factors of* $q^m - 1$ *divide* $q^n - 1$.

Then the sequence $\{u_t\}$ *in* $GF(q)$ *is of period* $(q^n - 1)(q^m - 1)$ *and linear complexity* $n(q^m - 1)$.

Proof. We will use the notation in Theorem 3.2. Note that

$$M = q^m - 1, \quad N = q^n - 1, \quad K = M + \frac{q^m(q^k - 1)}{2}$$

The condition (i) implies that $(N, K) = 1$. Hence $\{u_t\}$ is generated by $h(x^M) \in GF(q)[x]$, by Theorem 3.2.

On the other hand, since the conditions (ii) and (iii) hold, $h(x^M)$ is a monic irreducible polynomial in $GF(q)[x]$ of degree nM and order NM by Proposition 2.5.

Hence $h(x^M)$ is the minimum polynomial of $\{u_t\}$, and so $\{u_t\}$ is of period $(q^n - 1)(q^m - 1)$ and linear complexity $n(q^m - 1)$.

In the case when $q = 2$ Theorem 3.3 can be rewritten as the following corollary, which is the main theorem in [1].

COROLLARY 3.4. *Assume that $q = 2$ and the following two conditions hold.*

(i) $(2^n-1,\ 2^m-1+2^{m-1}(2^k-1)) = 1$.

(ii) *All prime factors of $2^m - 1$ divide $2^n - 1$.*

Then the sequence $\{u_t\}$ in $GF(2)$ is of period $(2^n-1)(2^m-1)$ and linear complexity $n(2^m - 1)$.

Now consider the case when $m = n$ in Theorem 3.3.

In Theorem 3.3, if $m = n$ then the conditions (ii) and (iii) are satisfied automatically, and the condition (i) is equivalent to the condition

$$(*) \qquad \left(q^n-1,\ \frac{q^n(q^{k-1})}{2}\right) = 1.$$

If q is even, then the condition $(*)$ is equivalent to the condition $(q^n - 1, q^k - 1) = 1$. Since $q^{(n,k)} - 1$ is a common divisor of $q^n - 1$ and $q^k - 1$, the condition $(q^n - 1, q^k - 1) = 1$ holds if and only if $q = 2$ and $(n, k) = 1$.

If q is odd, then $(*)$ is equivalent to the condition

$$(**) \qquad \left(q^n-1,\ \frac{q^k-1}{2}\right) = 1.$$

Now assume that q is odd and that the condition $(**)$ holds. Then $q^{(n,k)} - 1$ is divided by 2, and so $q = 3$ and $(n, k) = 1$. And k is odd if and only if $(3^k - 1)/2$ is odd. Therefore, if q is odd and the condition $(**)$ holds then $q = 3$, $(n, k) = 1$ and k is odd.

Conversely, assume that $q = 3, (n, k) = 1$ and k is odd. And suppose that there exists an odd prime p which divides both 3^n-1 and $(3^k-1)/2$. Then p is a common divisor of $3^n - 1$ and $3^k - 1$ and so

$$3^n \equiv 1 \pmod{p} \quad \text{and} \quad 3^k \equiv 1 \pmod{p}.$$

Let r be the order of 3 modulo p. Then the above congruences yield that $r|(n,k)$ and so $r=1$. This implies that $3 \equiv 1 \pmod{p}$ and $p=2$, which is a contradiction. Hence if $q=3$, $(n,k)=1$ and k is odd, then the condition $(**)$ holds.

Therefore, we obtain the following corollary.

COROLLARY 3.5. *Assume that $m=n$. Then the following hold.*

(1) *If $q=2$ and $(n,k)=1$, then the sequence $\{u_t\}$ in $GF(2)$ is of period $(2^n-1)^2$ and linear complexity $n(2^n-1)$.*

(2) *If $q=3$, $(n,k)=1$ and k is odd, then the sequence $\{u_t\}$ in $GF(3)$ is of period $(3^n-1)^2$ and linear complexity $n(3^n-1)$.*

References

1. Chambers, W. G. and S. M. Jennings, *Linear equivalence of certain BRM shift-register sequence,* Electronics Letters, **20**(1984), 149–152.
2. Jennings, S. M., *Multiplexed sequences: Some properties of the minimum polynomial,* Lecture Notes in Computer Science, Vol. **149**, Cryptography, Springer-Verlag, 1982.
3. Lidl, R., and H. Niederreiter, *Finite fields,* Encyclopedia of Mathematics and its application, Vol **20**, Addison-Wesley, Reading Mass, 1983.
4. Madden, D. J., *Polynomials and primitive roots in finite fields,* J. of Number theory, **13** (1981), 499-514.
5. Rueppel, R. A., and O. J. Staffbach, *Products of linear recurring sequences.*
6. Selmer, E., *Linear recurrence relations over finite fields,* University of Bergen, Norway, 1966.
7. Zieler, N. and N. H. Mills, *Products of linear recurring sequences,* J. of Algebra **27**(1973), 147–157.

DEPARTMENT OF MATHEMATICS, SOGANG UNIVERSITY, SEOUL 121-742, KOREA