Fast Algorithms for Determining the Minimal Polynomials of Sequences with Period kn over $GF(P^m)$

Jianqin Zhou
Department of Computer Science, Anhui University of Technology
Ma'anshan, Anhui 243002, China (Email: zhou9@yahoo.com)

(Received July 15, 2006; revised and accepted Oct. 3, 2006 & Nov. 8, 2006)

Abstract

A fast algorithm is derived for determining the linear complexity and the minimal polynomials of sequences over $GF(p^m)$ with period kn, where p is a prime number, $\gcd(n, p^m - 1) = 1$ and $p^m - 1 = ku, n, k$ and u are integers. The algorithm presented here covers the algorithm proposed by Chen for determining the minimal polynomials of sequences over $GF(p^m)$ with period $2^t n$, where p is a prime, $\gcd(n, p^m - 1) = 1$ and $p^m - 1 = 2^t u, n$ and u are integers. Combining our result with some known algorithms, it is possible to determine the linear complexity of sequences over $GF(p^m)$ with period kn more efficiently. Finally an example applying this algorithm is presented.

Keywords: Cryptography, linear complexity, minimal polynomial, stream cipher

1 Introduction

The concept of linear complexity is very useful in the study of the security of stream ciphers for cryptographic applications. A necessary condition for the security of a key stream generator is that it produces a sequence with large linear complexity. In [4], Games and Chan presented a fast algorithm for determining the linear complexity of a binary sequence with period 2^n. Ding, Xiao and Shan [3] and Blackburn [1] generalized the algorithm.

In [6], a fast algorithm for determining the linear complexity of a sequence with period p^n over $GF(q)$ was presented, where p is an odd prime, q is a prime and a primitive root modulo p^2. The algorithm makes up for the shortcoming that the Games-Chan algorithm cannot compute the linear complexity of sequences with period $N(\neq q^m)$ over $GF(q)$ in part. The time complexity and the space complexity of the algorithm are both $O(t)$, where $t = p^n$.

In [2], a result was presented to reduce the computation of the linear complexity of a sequence over $GF(p^m)$ (p is an odd prime) with period $2n$(n is a positive integer such that there exists an element $b \in GF(p^m), b^n = -1$) to the computation of the linear complexities of two sequences with period n. By combining this result with some known algorithms such as the Berlekamp-Massey algorithm and the Games-Chan algorithm, one can determine the linear complexity of a sequence with period $2^t n$ over $GF(p^m)$, where p is a prime, $\gcd(n, p^m - 1) = 1$ and $p^m - 1 = 2^t u, n$ and u are integers.

In this correspondence, a fast algorithm is derived for determining the minimal polynomial and the linear complexity of sequences over $GF(p^m)$ with period kn, where p is a prime, $\gcd(n, p^m - 1) = 1$ and $p^m - 1 = 2^t u, n, k$ and u are integers. The algorithm presented here covers the algorithm proposed by Hao Chen in [2]. Combining our result with some known algorithms, it is possible to determine the linear complexity of sequences over $GF(p^m)$ with period kn more efficiently.

In this correspondence, we consider sequences over $GF(p^m)$, where p is a prime. Let $s = \{s_0, s_1, s_2, s_3, \cdots\}$ be a sequence over $GF(p^m)$. If there exists a positive number N such that $s_i = s_{i+N}$ for $i = 0, 1, 2, \cdots$, then s is called a periodic sequence, and N is called a period of s.

The generated function of a sequence $s = \{s_0, s_1, s_2, s_3, \cdots, \}$ is defined by $s(x) = s_0 + s_1 x + s_2 x^2 + s_3 x^3 + \cdots = \sum_{i=0}^{\infty} s_i x^i$.

Let s be a periodic sequence with the first period $s^N = \{s_0, s_1, s_2, \cdots, s_{N-1}\}$. The generated function of s^N is defined by $s^N(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} x^{N-1}$. If

s is a periodic sequence with the first period s^N, then,

$$\begin{aligned} s(x) &= s^N(x)(1+x^N+x^{2N}+\cdots) \\ &= \frac{s^N(x)}{1-x^N} \\ &= \frac{s^N(x)/\gcd(s^N(x),1-x^N)}{(1-x^N)/\gcd(s^N(x),1-x^N)} \\ &= \frac{g(x)}{f_s(x)}, \end{aligned}$$

where $f_s(x) = (1-x^N)/\gcd(s^N(x), 1-x^N), g(x) = s^N(x)/\gcd(s^N(x), 1-x^N)$.

Obviously, $\gcd(g(x), f_s(x)) = 1$, $deg(g(x) < deg(f_s(x)))$. The polynomial $f_s(x)$ is called the minimal polynomial of s, and the degree of $f_s(x)$ is called the linear complexity of s, that is $deg(f_s(x)) = c(s)$ [6].

2 Main result

Lemma 1. *Let p be a prime, and $p^m - 1 = ku, k$ and u are all positive integers. If α is a generator of $GF(p^m)$, then*

1) $1 - x^k = \frac{1}{\alpha^u\alpha^{2u}\cdots\alpha^{(k-1)u}}(1-x)(\alpha^u - x)(\alpha^{2u} - x)\cdots(\alpha^{(k-1)u} - x)$;
2) *If* $\gcd(n, p^m - 1) = 1$, *then* α^n *is a generator of* $GF(p^m)$;
3) $\gcd(t(x), g(x)) = \gcd(\bar{t}(x), g(x))$, *where* $\bar{t}(x)$ *is the reduced polynomial of* $t(x)$ *modulo* $g(x)$, *i.e.,* $\bar{t}(x) \equiv t(x) \pmod{g(x)}$;
4) *Let* $g(x) = g_1(x)g_2(x)\cdots g_j(x)$, *where* g_i*'s are polynomials over* $GF(p^m)$ *which are pairwisely coprime (not necessarily irreducible over* $GF(p^m)$*). Then* $\gcd(t(x), g(x)) = \prod_{i=1}^{j} \gcd(t(x), g_i(x))$.

Proof.

1) Since $p^m - 1 = ku$, so $\alpha^{ku} = 1$, hence $1 - x^k = 0$ has roots: $1, \alpha^u, \alpha^{2u}, \cdots, \alpha^{(k-1)u}$.

   If k is odd, then $1 - x^k = (1-x)(\alpha^u - x)(\alpha^{2u} - x)\cdots(\alpha^{(k-1)u} - x)$, hence $\alpha^u\alpha^{2u}\cdots\alpha^{(k-1)u} = (-1)^{k-1}$.

   If k is even, then $1 - x^k = (-1)(1-x)(\alpha^u - x)(\alpha^{2u} - x)\cdots(\alpha^{(k-1)u} - x)$, hence $\alpha^u\alpha^{2u}\cdots\alpha^{(k-1)u} = (-1)^{k-1}$.

   Combining the above results, the identity is immediate.

2) Since $\gcd(n, p^m - 1) = 1$, if $\alpha^{ni} = 1$, then $(p^m - 1)|i$, hence $\alpha^n, \alpha^{2n}, \cdots, \alpha^{(p^m-1)n}$ are distinct. Thus α^n is a generator of $GF(p^m)$.

   The remaining of Lemma is immediate [5].

□

The following statement is the main result of this note, which reduces the computation of the linear complexity of a sequence over $GF(p^m)$ with period kn to the computation of the linear complexities of k sequences with period n.

Theorem 1. *Let $s = a_0, a_1, \cdots, a_{kn-1}, a_0, a_1, \cdots$ be a sequence over $GF(p^m)$ with period kn, where n, k and u are positive integers such that $\gcd(n, p^m - 1) = 1$ and $p^m - 1 = ku$. Let α be a generator of $GF(p^m)$, $\beta = \alpha^u$.*

For $1 \le i \le k$, let $s_{(i)}$ be a sequence over $GF(p^m)$ with period n and its first period $s^n_{(i)} = \{s_{(i),0}, s_{(i),1}, s_{(i),2}, \cdots, s_{(i),n-1}\}$, where $s_{(i),v} = \{s_v + s_{n+v}(\beta^{i-1})^{n+v} + \cdots + s_{(k-1)n+v}(\beta^{i-1})^{(k-1)n+v}, 0 \le v < n$.

Then $\gcd(s^{kn}(x), 1 - x^{kn}) = \gcd(s^n_{(1)}(x), 1 - x^n)\gcd[s^n_2(\frac{x}{\beta^{2-1}}), 1 - (\frac{x}{\beta^{2-1}})^n]\cdots\gcd[s^n_{(k)}(\frac{x}{\beta^{k-1}}), 1 - (\frac{x}{\beta^{k-1}})^n]$.

Proof. From the above Lemma, we have, $1 - x^k = \frac{1}{\alpha^u\alpha^{2u}\cdots\alpha^{(k-1)u}}(1-x)(\alpha^u - x)(\alpha^{2u} - x)\cdots(\alpha^{(k-1)u} - x)$.

Since $\gcd(n, p^m - 1) = 1$, hence α^n is also a generator of $GF(p^m)$. So,

$$\begin{aligned} & 1 - x^{kn} = 1 - (x^n)^k \\ = & \frac{1}{\alpha^{nu}\alpha^{n2u}\cdots\alpha^{n(k-1)u}}(1-x^n)(\alpha^{nu} - x^n) \\ & (\alpha^{n2u} - x^n)\cdots(\alpha^{n(k-1)u} - x^n) \\ = & (1-x^n)(1-(\frac{x}{\alpha^u})^n)(1-(\frac{x}{\alpha^{2u}})^n)\cdots(1-(\frac{x}{\alpha^{(k-1)u}})^n) \\ = & \prod_{i=0}^{k-1}(1-(\frac{x}{\beta^i})^n). \end{aligned}$$

Thus,

$$\begin{aligned} & \gcd(s^{kn}(x), 1 - x^{kn}) \\ = & \gcd(s^{kn}(x), 1 - x^n)\gcd(s^{kn}(x), 1 - (\frac{x}{\beta})^n) \\ & \gcd(s^{kn}(x), 1 - (\frac{x}{\beta^2})^n)\cdots\gcd(s^{kn}(x), 1 - (\frac{x}{\beta^{k-1}})^n) \\ = & \prod_{i=0}^{k-1}\gcd(s^{kn}(x), 1 - (\frac{x}{\beta^i})^n). \end{aligned}$$

On the other side,

$$\begin{aligned} s^{kn}(x) &= s_0 + s_1x + s_2x^2 + \cdots + s_{kn-1}x^{kn-1} \\ &= x^0[s_0 + s_nx^n + s_{2n}x^{2n} + \cdots + s_{(k-1)n}x^{(k-1)n}] \\ &\quad + x^1[s_1 + s_{n+1}x^n + s_{2n+1}x^{2n} + \cdots \\ &\quad + s_{(k-1)n+1}x^{(k-1)n}] + \cdots + x^{n-1}[s_{n-1} \\ &\quad + s_{2n-1}x^n + s_{3n-1}x^{2n} + \cdots + s_{kn-1}x^{(k-1)n}]. \end{aligned}$$

Now it is obvious that,

$$\begin{aligned}&[s_0 + s_n x^n + s_{2n} x^{2n} + \cdots + s_{(k-1)n} x^{(k-1)n}] \bmod (1-x^n)\\ = \ &[s_0 + s_n + s_{2n} + \cdots + s_{(k-1)n}];\end{aligned}$$

$$\begin{aligned}&[s_1 + s_{n+1} x^n + s_{2n+1} x^{2n} + \cdots + s_{(k-1)n+1} x^{(k-1)n}] \bmod (1-x^n)\\ = \ &[s_1 + s_{n+1} + s_{2n+1} + \cdots + s_{(k-1)n+1}];\\ &\cdots\cdots\\ &[s_{n-1} + s_{2n-1} x^n + s_{3n-1} x^{2n} + \cdots + s_{kn-1} x^{(k-1)n}] \bmod (1-x^n)\\ = \ &[s_{n-1} + s_{2n-1} + s_{3n-1} + \cdots + s_{kn-1}].\end{aligned}$$

Thus $\gcd(s^{kn}(x), 1-x^n) = \gcd(s^n_{(1)}(x), 1-x^n)$.

For $i = 1, 2, \cdots, k-1$, with a similar argument, the computation of factor, $g_i(x) = \gcd(s^{kn}(x), 1-(\frac{x}{\beta^i})^n))$ is worked out with the change of variable $y = \frac{x}{\beta^i}$. So we have, $s^{kn}(\beta^i y) \bmod (1-y^n) = s^n_{(i)}(y)$.

Thus, $g_i(x) = \gcd(s^{kn}(\beta^i y), 1-y^n) = \gcd(s^n_{(i)}(y), 1-y^n) = \gcd(s^n_{(i)}(\frac{x}{\beta^i}), 1-(\frac{x}{\beta^i})^n)$. □

As multiplication over $GF(p^m)$ takes much longer time than addition, thus additions are ignored concerning the complexity analysis. For $i(1 < i \leq k)$, the reduction needs less than $2kn$ field multiplication operations to compute $s_j(\beta^{i-1})^j (0 < j < kn)$. Thus, the total number of multiplication operations of the reduction is less than $2(k-1)(kn)$, where kn is the period of the original sequence.

3 Fast Algorithm

Note that with the condition $\gcd(n, p^m - 1) = 1$ and $p^m - 1 = ku$, where n, k and u are positive integers, we may combine the theorem above with some known algorithms to give some fast algorithms to compute the minimal polynomial and the linear complexity of a sequence over $GF(p^m)$ with period kn.

Combining the theorem above with the algorithm proposed in [6], we now give a fast algorithm to compute the linear complexity of sequences over $GF(p)$ with period $kq^m (p-1 = ku)$ in the complexity $O(kq^m)$. Here we need the storage of one generator of $GF(p)$ in advance.

Algorithm: Let $s = (s_0, s_1, s_2 \cdots)$ be a sequence over $GF(p)$ with period $N = kq^m$, where $p-1 = ku, p$ and q are primes and p is a primitive root modulo q^2, and $s^N = (s_0, s_1, \cdots, s_{N-1})$ be the first period of s.

1) Initial values: α is a generator of $GF(p), \beta = \alpha^u, c = 0, f = 1$.

2) Loop: for $1 \leq i \leq k, n = q^m$, to compute $s^n_{(i)} = \{s_{(i),0}, s_{(i),1}, s_{(i),2}, \cdots, s_{(i),n-1}\}$, where $s_{(i),v} = \{s_v + s_{n+v}(\beta^{i-1})^{n+v} + \cdots + s_{(k-1)n+v}(\beta^{i-1})^{(k-1)n+v}, 0 \leq v < n$.

   Call Function, $c = c(s^n_{(i)}) + c; f = f \cdot f^n_{(i)}(\frac{x}{\beta^{i-1}})$.

3) End. The linear complexity of s is c; the minimal polynomial of s is f.

Function:

1) Initial values: $a = (a_0, a_1, \cdots, a_{n-1})$ is the first period of $s, n = q^m, c = 0, f = 1$.

2) If $a = (0, \cdots, 0)$, then end; If $n = 1$, then $c = c + 1, f = (1-x)f$, end.

3) $n = n/q$, let $A_i = (a_{(i-1)n}, a_{(i-1)n+1}, \cdots, a_{in-1}), i = 1, 2, \cdots, q$.

4) If $A_1 = A_2 = \cdots = A_q$, then $a = A_1$; else, $a = A_1 + A_2 + \cdots + A_q, c = c + (q-1)n, f = f\Phi_{qn}(x)$.

5) Goto 1).

6) End. The linear complexity of s is c; the minimal polynomial of s is f.

Note that the function above is just the algorithm for sequences over $GF(p)$ (see [6]).

Example 1. *Let the first period of s be S^{36} =124130140 040322412 034210224 030211402 over $GF(5)$. This is a sequence with period 4×3^2 over $GF(5)$. Since 5 is a primitive root modulo 3^2, $4|(5-1)$ and gcd$(3^2, 5-1)$=1, we may apply the algorithm above for determining the minimal polynomial and the linear complexity of s as follows:*

Since 2 is a generator of $GF(5)$, thus

$$\begin{aligned}s^9_{(1)} &= 123323123;\\ s^9_{(2)} &= 120344121, \beta = 2;\\ s^9_{(3)} &= 123213000, \beta^2 = 4;\\ s^9_{(4)} &= 110404101, \beta^3 = 3.\end{aligned}$$

For $s^9_{(1)} = 123323123$, call function.

Step 1. *A1=123, A2=323, A3=123; Since A1≠ A2, $n = 3$, thus $c = 6, f = \Phi_9(x), a = 014$;*

Step 2. *A1=0, A2=1, A3=4;*

Since A1≠ A2, $n = 1$, thus $c = 6 + 2 = 8, f = \Phi_9(x)\Phi_3(x), a = 0$; stop.

For $s^9_{(2)} = 120344121$, call function.

Step 1. *A1=120, A2=344, A3=121;*

Since A1≠ A2, n=3, thus $c = 6, f = \phi_9(x), a = 030$;

Step 2. *A1=0, A2=3, A3=0;*

Since A1≠ A2, n=1, thus $c = 6 + 2 = 8, f = \phi_9(x)\phi_3(x)$, a=3;

Step 3. $c = 8 + 1 = 9, f = \phi_9(x)\phi_3(x)(1 - x)$, *stop.*

For $s^9_{(3)}$ *=123213000, call function.*

Step 1. *A1=123, A2=213, A3=000;*

Since A1≠ A2, n=3, thus $c = 6, f = \phi_9(x), a = 331$*;*

Step 2. *A1=3, A2=3, A3=1;*

Since A1≠A3, n=1, thus $c = 6 + 2 = 8, f = \phi_9(x)\phi_3(x), a = 2$*;*

Step 3. $c = 8 + 1 = 9, f = \phi_9(x)\phi_3(x)(1 - x)$, *stop.*

For $s^9_{(4)} = 110404101$, *call function.*

Step 1. *A1=110, A2=404, A3=101;*

Since A1≠A2, n=3, thus $c = 6, f = \phi_9(x), a = 110$*;*

Step 2. *A1=1, A2=1, A3=0;*

Since A1≠A3, n=1, thus $c = 6 + 2 = 8, f = \phi_9(x)\phi_3(x), a = 2$*;*

Step 3. $c = 8 + 1 = 9, f = \phi_9(x)\phi_3(x)(1 - x)$, *stop.*

Finally, the linear complexity of s is 35, the minimal polynomial is

$$\begin{aligned} f_s &= \phi_9(x)\phi_3(x)\phi_9(x/2)\phi_3(x/2)(1 - x/2) \\ &\quad \phi_9(x/4)\phi_3(x/4)(1 - x/4)\phi_9(x/3)\phi_3(x/3)(1 - x/3) \\ &= \phi_9(x)\phi_3(x)\phi_9(3x)\phi_3(3x)(1 - 3x) \\ &\quad \phi_9(4x)\phi_3(4x)(1 - 4x)\phi_9(2x)\phi_3(2x)(1 - 2x), \end{aligned}$$

where the last equality follows by the fact that $2 \times 3 = 1, 4 \times 4 = 1$ *over* $GF(5)$.

4 Conclusion

We have proved a result reducing the computation of the linear complexity of sequences over $GF(p^m)$ with period kn (where p is a prime and n is a positive integer such that $\gcd(n, p^m - 1)$=1 and $p^m - 1 = ku$) to the computation of the linear complexities of k sequences with period n. Combining this reduction with some known algorithms, we can compute the linear complexity of sequences with period kn ($\gcd(n, p^m - 1)$=1 and $p^m - 1 = ku$) over $GF(p^m)$ more efficiently.

Acknowledgments

The author wishes to thank the anonymous referees for many constructive comments that significantly improved the presentation of this paper. The research is supported by Natural Science Foundation of Anhui Education Bureau (No. 2006KJ238B)

References

[1] S. R. Blackburn, "A generalization of the discrete Fourier transform: Determining the minimal polynomial of a periodic sequence," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1702-1704, 1994.

[2] H. Chen, "Fast algorithms for determining the linear complexity of sequences over $GF(p^m)$ with period $2^t n$," *IEEE Transactions on Information Theory*, vol. 51, no. 5, pp. 1854-1856, 2005.

[3] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, pp. 85-88, Springer-Verlag, 1991.

[4] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 144-146, 1983.

[5] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, 1987.

[6] G. Z. Xiao, S. M. Wei, K. Y. Lam, and K. Imamura, "A fast algorithm for determining the linear complexity of a sequence with period p^n over $GF(q)$," *IEEE Transactions on Information Theory*, vol. 46, no. 6, pp. 2203-2206, 2000.

Jianqin Zhou received his B.Sc. degree in mathematics from East China Normal University, China, in 1983, and M.Sc. degree in probability and statistics from Fudan University, China. From 1989 to 1999 he was with the Department of Mathematics and Computer Science, Qufu Normal University, China. From 2000 to 2002, he worked for a number of IT companies in Japan. Since 2003 he has been with the Department of Computer Science, Anhui University of Technology, China. From Sep 2006 to Feb 2007, he was a visiting scholar with the Department of Information and Computer Science, Keio University, Japan. He published more than thirty five papers, and proved a conjecture posed by famous mathematician Paul Erdös et al. His research interests include coding theory, cryptography and combinatorics.