A Fast Algorithm for Determining the Linear Complexity of Periodic Sequences over $GF(3)^\star$

Jianqin Zhou** and Qiang Zheng

Dept. of Computer Science, Anhui Univ. of Technology, Ma'anshan 243002, China
zhou9@yahoo.com

Abstract. A fast algorithm is derived for determining the linear complexity and the minimal polynomial of periodic sequences over $GF(3)$ with period $3^n p^m$, where p is a prime number, and 3 is a primitive root modulo p^2 . The algorithm presented here generalizes the fast algorithm to determine the linear complexity of a sequence over $GF(q)$ with period p^m, where p is a prime, q is a prime and a primitive root modulo p^2.

Keywords: Cryptography; periodic sequence; linear complexity; minimal polynomial.

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. Games-Chan algorithm in [1] was proposed to compute the linear complexity of sequences over $GF(2)$ with period 2^n , and was generalized to the sequences over $GF(p^m)$ with period p^n , where p is a prime, by Ding, Xiao and Shan in [2]. Wei, Xiao and Chen in [4] presented an algorithm to compute the linear complexity of sequences over $GF(q)$ with period p^m , where p is a prime, q is a prime and a primitive root modulo p^2. They in [5] presented an algorithm to compute the linear complexity of sequences over $GF(2)$ with period $2^n p^m$, where 2 is a primitive root modulo p^2.

In this paper, a fast algorithm is derived for determining the linear complexity and the minimal polynomial of periodic sequences over $GF(3)$ with period $3^n p^m$, where p is a prime, 3 is a primitive root modulo p^2. A numerical example is presented to illustrate the new algorithm. The algorithm presented here generalizes both the algorithm in [4] where the period of a sequence over $GF(q)$ is p^m and the algorithm in [5] where the period of a binary sequence is $2^n p^m$. With an approach similar to the case that $q = 3$ as described here, it is easy to derive a fast algorithm for determining the linear complexity and the minimal polynomial of periodic sequences over $GF(q)$ with period $q^n p^m$, where p is a prime, q is a prime and is a primitive root modulo p^2.

⋆ The research is supported by Natural Science Foundation of Anhui Education Bureau (No. 2006KJ238B).

⋆⋆ Corresponding author.

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 213–223, 2006.

1 Preliminaries

For the definitions and lemmas presented here, we refer to [4,5] and the relevant references given in them.

We will consider sequences over $GF(3)$. Let $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ be vectors over $GF(3)$. Then define $x + y = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$.

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

The generated function of a finite sequence $s^N = \{s_0, s_1, s_2, \cdots, s_{N-1}, \}$ 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, $gcd(g(x), f_s(x)) = 1, deg(g(x) < deg(f_s(x)))$. $f_s(x)$ is called the minimal polynomial of s, and the degree of $f_s(x)$ is called the linear complexity of s, that is $deg(f_s(x)) = c(s)$[2].

Let us recall some results in finite field theory[8] and number theory[9].

Definition 1.1. Let n be a positive integer. The polynomial $\Phi_n(x) = \Pi_{0<j<n,(j,n)=1}(x - \xi_n^j)$, where ξ_n is a n-th primitive unit root, and $(j, n) = 1$ denotes j is relatively prime to n, is called the n-th cyclotomic polynomial.

Lemma 1.1. Let p be a prime. Then $\varphi(p^n) = p^n - p^{n-1}$, where n is a positive integer, φ is the Euler function.

Lemma 1.2. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial. Then $\Phi_n(x)$ is irreducible over $GF(3)$ if and only if that 3 is a primitive root modulo n, that is the order of 3 modulo n is $\varphi(n)$.

Lemma 1.3. Let p be a prime and m a positive integer. Then $\Phi_{p^m}(x) = \Phi_p(x^{p^{m-1}})$.

Lemma 1.4. Let p be a prime, m and n be positive integers. Let $\Phi_{p^m}(x)^{3^n}$ denote $[\Phi_{p^m}(x)]^{3^n}$. Then $\Phi_{p^m}(x)^{3^n} = \Phi_{p^m}(x^{3^n}) = \Phi_p(x^{3^n p^{m-1}})$, where the operation is over $GF(3)$.

Lemma 1.5. Let p be a prime, 3 be a primitive root modulo p^2. Then 3 is a primitive root modulo p^n , $n \geq 1$, so $\Phi_{p^n}(x)$ is irreducible over $GF(3)$.

2 Main Theorems Concerning Algorithms

The following lemma and its proof are from [4].