Journal of Southeast University (English Edition) Vol. 28, No. 3, pp. 367 – 371 Sept. 2012 ISSN 1003—7985

Fast algorithm for determining the minimal polynomial of up^n -periodic sequence

Hu Weiqun[1] Yue Qin[2]

([1]College of Science, Nanjing Forestry University, Nanjing 210037, China)
([2]College of Science, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: A fast algorithm for determining the minimal polynomial and linear complexity of a up^n-periodic sequence over a finite field F_q is given. Let p, q, and u be distinct primes, q a primitive root modulo p^2, m the smallest positive integer such that $q^m \equiv 1 \bmod u$, and $\gcd(m, p(p-1)) = 1$. An algorithm is used to reduce a periodic up^n sequence over F_q to several p^n-periodic sequences over $F_q(\zeta)$, where ζ is a u-th primitive root of unity, and an algorithm proposed by Xiao et al. is employed to obtain the minimal polynomial of each p^n-periodic sequence.

Key words: minimal polynomial; linear complexity; periodic sequence

doi: 10.3969/j.issn.1003 – 7985.2012.03.020

Let $s = \{s_0, s_1, \ldots, s_{N-1}, s_0, s_1, \ldots\}$ be an N-periodic sequence over a finite field $F_q = \mathrm{GF}(q)$, we define that its linear complexity $c(s)$ is the length of the shortest linear feedback shift register to generate it; i.e., the smallest positive integer k such that there exist some c_1, c_2, …, c_k in F_q with $s_{i+k} = c_1 s_{i+k-1} + \ldots + c_k s_i$ for all $i \geqslant 0$. We call the polynomial $m(s) = 1 - (c_1 x + \ldots + c_k x^k)$ the minimal polynomial of the sequence s.

The linear complexity of a periodic sequence plays an important role in the application of the sequence in cryptography and communication. There are a lot of papers[1–10] on efficient algorithms for determining the linear complexity and minimal connection polynomials of sequences. The famous Berlekamp-Massey algorithm[8] can be used to compute the linear complexity and minimal polynomial of an N-periodic sequence over F_q with time complexity $O(N^2)$, i.e., at most $O(N^2)$ of field operations in F_q.

There have been some results to determine the linear complexity and minimal polynomial of an N-periodic sequence over F_q with time complexity $O(N)$ under the following conditions:

1) $N = 2^n$, $q = 2$[6].

2) $N = p^n$, $q = p^m$[4].

3) $N = p^n$, where q is a prime, a primitive root modulo p^2[10]; $N = 2p^n$, where q is an odd prime, a primitive root modulo p^2[8].

4) $N = 2^t n$, $q = p^m$, $2^t \mid p^m - 1$, $\gcd(n, p^m - 1) = 1$[2]; $N = un$, $q = p^m$, $u \mid p^m - 1$, $\gcd(n, p^m - 1) = 1$[3].

In general, the time complexity of the algorithm in Refs. [2 – 3] is not $O(N)$. Only when n is special may the time complexity be $O(N)$. See Refs. [2 – 3] for details.

For a sequence $s = \{s_0, s_1, \ldots, s_{N-1}, s_0, \ldots\}$ over F_q, its generating function is

$$s(x) = s_0 + s_1 x + s_2 x^2 + \ldots$$

Let s be an N-periodic sequence with the first period $(s_0, s_1, \ldots, s_{N-1})$ and

$$s^N(x) = s_0 + s_1 x + \ldots + s_{N-1} x^{N-1}$$

Then the linear complexity of the sequence s is

$$c(s) = \deg(1 - x^N) - \deg(\gcd(1 - x^N, s^N(x))$$

and the minimal polynomial is

$$f_s(x) = \frac{1 - x^N}{\gcd(1 - x^N, s^N(x))}$$

1 Main Result

In this paper, we always assume that p, q, and u are distinct primes; q is a primitive root modulo p^2; m is the smallest positive integer such that $q^m \equiv 1 \bmod u$ (i.e. m is called the order of q modulo u) and $\gcd(m, p(p-1)) = 1$.

We recall some results in finite field and number theory. Let K be a field of character q, $\gcd(q, n) = 1$, and ζ the n-th primitive root of unity. Then

$$\Phi_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \zeta^s)$$

is called the n-th cyclotomic polynomial over K. It is a well-known fact that $\Phi_n(x)$ is irreducible in F_q if and only if q is a primitive root modulo n, i.e., q has order $\phi(n)$ modulo n, where $\phi(n)$ is the Euler-function[7].

Now we recall a result in Ref. [10].

Received 2011-11-18.

Biography: Hu Weiqun (1958—), female, professor, huweiqun@njfu.edu.cn.

Foundation item: The National Natural Science Foundation of China (No. 10971250, 11171150).

Citation: Hu Weiqun, Yue Qin. Fast algorithm for determining the minimal polynomial of up^n-periodic sequence[J]. Journal of Southeast University (English Edition), 2012, 28(3): 367 – 371. [doi: 10.3969/j.issn.1003 – 7985.2012.03.020]

Lemma 1 Let p, q be distinct primes and q a primitive root $(\mathrm{mod}\ p^2)$. Let s be a p^n-periodic sequence over F_q with the first period $(s_0, s_1, \ldots, s_{p^n-1})$. Set

$$A_i = (s_{(i-1)p^{n-1}}, \ldots, s_{ip^{n-1}-1}) \qquad i = 1, 2, \ldots, p$$

1) If $A_1 = A_2 = \ldots = A_p$, then $f_s(x) = f_a(x)$, $c(s) = c(a)$, where a is a p^{n-1}-periodic sequence with the first period A_1.

2) Otherwise, $f_s(x) = f_b(x)\Phi_{p^n}(x)$, $c(s) = c(b) + (p-1)p^{n-1}$, where b is a p^{n-1}-periodic sequence with the first period $A_1 + A_2 + \ldots + A_p$.

It is known that when q is a primitive root modulo p, then q or $p+q$ is a primitive root modulo p^2. Suppose that q is a primitive root modulo p^2, then q is a primitive root modulo $p^n (n \geqslant 1)$.

In this paper, we always assume that q is a primitive root modulo p^2, so $\Phi_{p^n}(x)$ is an irreducible polynomial over F_q. Suppose that m is the order of q modulo u, then $u \mid q^m - 1$. There is a u-th primitive root $\zeta \in F_{q^m}$ and $F_q(\zeta) = F_{q^m}$ (see Theorem 2.47 in Ref. [7]). There are several equalities:

$$1 - x^u = \prod_{j=0}^{u-1}(1 - \zeta^{-j}x)$$

$$1 - x^{up^n} = \prod_{j=0}^{u-1}(1 - (\zeta^{-j}x)^{p^n})$$

$$1 - (\zeta^{-j}x)^{p^n} = (1 - (\zeta^{-j}x)^{p^{n-1}})\Phi_{p^n}(\zeta^{-j}x)$$

where $\Phi_{p^n}(x) = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \ldots + 1 = \Phi_p(x^{p^{n-1}})$.

We state a result in Ref. [3].

Lemma 2 Let p, q, u, and m be defined as above. Let $s = \{s_0, s_1, \ldots\}$ be an $N(= up^n)$-periodic sequence over F_q with the first period $(s_0, s_1, \ldots, s_{N-1})$. Let $s^{(j)}$ be the p^n-periodic sequence over F_{q^m} with the first period $(s_0^{(j)}, s_1^{(j)}, \ldots, s_{p^n-1}^{(j)})$, $s_0^{(j)} = s_0 + s_{p^n}\zeta^{jp^n} + \ldots + s_{(u-1)p^n}\cdot\zeta^{j(u-1)p^n}$, $\ldots$, $s_i^{(j)} = s_i\zeta^{ji} + s_{p^n+i}\zeta^{j(p^n+i)} + \ldots + s_{(u-1)p^n+i}\cdot\zeta^{j((u-1)p^n+i)}$, $\ldots$, $s_{p^n-1}^{(j)} = s_{p^n-1}\zeta^{j(p^n-1)} + s_{2p^n-1}\zeta^{j(2p^n-1)} + \ldots + s_{up^n-1}\zeta^{j(up^n-1)}$ for $j = 0, 1, \ldots, u-1$.

1) Then

$$f_s(x) = f_{s^{(0)}}(x)f_{s^{(1)}}(\zeta^{-1}x)\ldots f_{s^{(u-1)}}(\zeta^{-u+1}x) \in F_q(x)$$
$$c(s) = c(s^{(0)}) + c(s^{(1)}) + \ldots + c(s^{(u-1)})$$

where $f_{s^{(j)}}(\zeta^{-j}x) \in F_{q^m}(x)$ for $j = 0, 1, 2, \ldots, u-1$.

2) For each sequence $s^{(j)}$, set

$$A_i^{(j)} = (s_{(i-1)p^{n-1}}^{(j)}, \ldots, s_{ip^{n-1}-1}^{(j)}) \qquad i = 1, 2, \ldots, p$$

a) $A_1^{(j)} = A_2^{(j)} = \ldots = A_p^{(j)}$, then

$$f_{s^{(j)}}(\zeta^{-j}x) = f_{a^{(j)}}(\zeta^{-j}x), \quad c(s^{(j)}) = c(a^{(j)})$$

where $a^{(j)}$ is the p^{n-1}-periodic sequence over F_{q^m} with the first period $A_1^{(j)}$.

b) Otherwise,

$$f_{s^{(j)}}(\zeta^{-j}x) = f_{b^{(j)}}(\zeta^{-j}x)\Phi_{p^n}(\zeta^{-j}x)$$
$$c(s^{(j)}) = c(b^{(j)}) + p^{n-1}(p-1)$$

where $b^{(j)}$ is the p^{n-1}-periodic sequence with the first period $A_1^{(j)} + A_2^{(j)} + \ldots + A_p^{(j)}$.

Proof For completion, we give a simple proof. Let $s^N(x) = \sum_{i=0}^{up^n-1} s_i x^i$ and $1 - x^{up^n} = \prod_{j=0}^{u-1}(1 - (\zeta^{-j}x)^{p^n})$, then $\gcd(u, p^n) = 1$, $\gcd(1 - (\zeta^{-i}x)^{p^n}, 1 - (\zeta^{-j}x)^{p^n}) = 1$ if $i \neq j$. Hence $\gcd(s^N(x), 1 - x^{up^n}) = \prod_{j=0}^{u-1}\gcd(s^N(x), 1 - (\zeta^{-j}x)^{p^n})$. In F_{q^m},

$$s^N(x) = \sum_{i=0}^{up^n-1} s_i x^i + \zeta^{jp^n}\Big(\sum_{i=p^n}^{2p^n-1} s_i x^{i-p^n}\Big)(\zeta^{-j}x)^{p^n} + \ldots + \zeta^{j(u-1)p^n}\Big(\sum_{i=(u-1)p^n}^{up^n-1} s_i x^{i-(u-1)p^n}\Big) = ((\zeta^{-j}x)^{p^n} - 1)g(x) + r_j(x)$$

where $g(x) \in F_{q^m}[x]$ and $r_j(x) = s^{(j)}(\zeta^{-j}x) = \sum_{i=0}^{p^n-1} s_i^{(j)}\cdot(\zeta^{-j}x)^i = \sum_{i=0}^{p^n-1} s_i x^i + \zeta^{jp^n}\Big(\sum_{i=p^n}^{2p^n-1} s_i x^{i-p^n}\Big) + \ldots + \zeta^{j(u-1)p^n}\cdot\Big(\sum_{i=(u-1)p^n}^{up^n-1} s_i x^{i-(u-1)p^n}\Big) \in F_{q^m}[x]$. Hence $\gcd(s^N(x), 1 - (\zeta^{-j}x)^{p^n}) = \gcd(s^{(j)}(\zeta^{-1}x), 1 - (\zeta^{-j}x)^{p^n})$. So

$$f_{s^{(j)}}(\zeta^{-j}x) = \frac{1 - (\zeta^{-j}x)^{p^n}}{\gcd(s^{(j)}(\zeta^{-j}x), 1 - (\zeta^{-j}x)^{p^n})}$$
$$j = 0, 1, \ldots, u-1$$

We have $f_s(x) = f_{s^{(0)}}(x)f_{s^{(1)}}(\zeta^{-1}x)\ldots f_{s^{(u-1)}}(\zeta^{-u+1}x)$ and $c(s) = c(s^{(0)}) + c(s^{(1)}) + \ldots + c(s^{(u-1)})$.

Since q is a primitive root modulo p^2, $\Phi_{p^n}(x)$ is irreducible over F_q. Let ξ be a p^n-th primitive root of unity, $K = F_{q^m}(\xi)$ and $l = [K: F_q]$. Since $F_q \subset F_{q^m} \subset K$ and $F_q \subset F_q(\xi) \subset K$, $m \mid l$ and $p^{n-1}(p-1) \mid l$, but $\gcd(m, p^{n-1}(p-1)) = 1$. Hence $mp^{n-1}(p-1) \mid l$, so $l = mp^{n-1}(p-1)$ and $\Phi_{p^n}(x)$, $\Phi_{p^n}(\zeta^{-1}x)$, $\ldots$, $\Phi_{p^n}(\zeta^{-u+1}x)$ are irreducible over F_{q^m}.

For each sequence $s^{(j)}$ $(0 \leqslant j \leqslant u-1)$, the generating function of $A_i^{(j)}$ is as follows:

$$A_i^{(j)}(x) = \sum_{k=0}^{p^{n-1}-1} s_{(i-1)p^{n-1}+k}^{(j)} x^k \qquad i = 1, 2, \ldots, p$$

Thus the generating function of $s^{(j)}$ is

$$s^{(j)p^n}(x) = A_1^{(j)}(x) + x^{p^{n-1}}A_2^{(j)}(x) + \ldots + x^{(p-1)p^{n-1}}A_p^{(j)}(x)$$

1) If $A_1^{(j)} = A_2^{(j)} = \ldots = A_p^{(j)}$, then

$$s^{(j)p^n}(x) = A_1^{(j)}(x) + x^{p^{n-1}}A_1^{(j)}(x) + \ldots + x^{(p-1)p^{n-1}}A_1^{(j)}(x) = A_1^{(j)}(x)\Phi_{p^n}(x)$$

Hence

$$f_{s^{(j)}}(\zeta^{-j}x) = \frac{1 - (\zeta^{-j}x)^{p^n}}{\gcd(1 - (\zeta^{-j}x)^{p^n}, s^{(j)p^n}(\zeta^{-j}x))} =$$

$$\frac{1-(\zeta^{-j}x)^{p^n}}{\gcd(1-(\zeta^{-j}x)^{p^{n-1}}, A_1^{(j)}(\zeta^{-j}x))}=f_{a^{(j)}}(\zeta^{-j}x)$$

where $a^{(j)}$ is the p^{n-1}-periodic sequence over F_{q^m} with the first period $A_i^{(j)}$.

2) If $A_1^{(j)}=\ldots=A_p^{(j)}$ does not hold, then we have

$$\gcd(s^{(j)p^n}(\zeta^{-j}x),\ \Phi_{p^n}(\zeta^{-j}x))=1 \qquad (1)$$

Suppose that (1) does not hold, then by $\Phi_{p^n}(x)$ irreducible over F_{q^m} we have $\gcd(s^{(j)p^n}(\zeta^{-j}x),\ \Phi_{p^n}(x))=\Phi_{p^n}(x)$.

Set $s^{(j)p^n}(x)=q(x)\Phi_{p^n}(x)$, then

$$(A_1^{(j)}(x)-q(x))+(A_2^{(j)}(x)-q(x))x^{p^{n-1}}+\ldots+(A_p^{(j)}(x)-q(x))x^{(p-1)p^{n-1}}=0$$

From

$$\deg s^{(j)p^n}(x)\leqslant p^n-1,\ \deg\Phi_{p^n}(x)=(p-1)p^{n-1}$$

it follows that $\deg q(x)\leqslant p^{n-1}-1$. Clearly, $\deg A_i^{(j)}(x)\leqslant p^{n-1}-1$. Hence $A_1^{(j)}(x)=\ldots=A_p^{(j)}(x)=q(x)$, which is contradictory.

From (1) we have

$$\gcd(1-x^{p^n},\Phi_{p^n}(x))=\gcd((1-x^{p^{n-1}})\Phi_{p^n}(x)\ s^{(j)p^n}(x))=\gcd(1-x^{p^{n-1}},s^{(j)p^n}(x))$$

Since

$$s^{(j)p^n}(x)=A_2^{(j)}(x)(x^{p^{n-1}}-1)+\ldots+A_p^{(j)}(x)(x^{(p-1)p^{n-1}}-1)+(A_1^{(j)}(x)+\ldots+A_p^{(j)}(x))$$

we have

$$\gcd(1-x^{p^{n-1}},s^{(j)p^n}(x))=\gcd(1-x^{p^{n-1}},A_1^{(j)}(x)+\ldots+A_p^{(j)}(x))$$

Therefore

$$f_{s^{(j)}}(\zeta^{-j}x)=\frac{1-(\zeta^{-j}x)^{p^n}}{\gcd(1-(\zeta^{-j}x)^{p^n},s^{(j)p^n}(\zeta^{-1}x))}=\frac{(1-(\zeta^{-1}x)^{p^{n-1}})\Phi_{p^n}(\zeta^{-1}x)}{\gcd(1-(\zeta^{-1}x)^{p^{n-1}},A_1^{(j)}(\zeta^{-j}x)+\ldots+A_p^{(j)}(\zeta^{-j}x))}=\Phi_{p^n}(\zeta^{-1}x)f_{b^{(j)}}(\zeta^{-1}x)$$

where $b^{(j)}$ is the p^{n-1}-periodic sequence with the first period $A_1^{(j)}+\ldots+A_p^{(j)}$.

Since u is a prime, there is a factorization in F_q.

$$1-x^u=(1-x)\Phi_u(x)=(1-x)\Psi_1(x)\ldots\Psi_t(x) \qquad (2)$$

where each $\Psi_k(x)$ is irreducible and its scale term is 1. Let ζ be a u-th primitive root and ζ^{j_k} a root of $\Psi_k(x)$, $j_k\in\mathbf{Z}$, for $k=1,2,\ldots,t$. We have a lemma.

Lemma 3 Let p, q, u and m be defined as above. Then in (2), $\deg\Psi_k(x)=m$, $F_q(\zeta^{j_k})=F_{q^m}$ for $k=1,2,\ldots,t$ and $t=(u-1)/m$. Moreover there are permutations $\tau_n(n\geqslant 1)$: $\{1,2,\ldots,t\}\to\{1,2,\ldots,t\}$, $k\to h$, where ζ^{j_k} is a root of $\Psi_k(x)$, $\zeta^{j_kp^n}$ is a root of $\Psi_h(x)$, and $\tau_0=I$ is the identity permutation, such that

$$\Theta_{p^n}^{(k)}(x)=N_{F_{q^n}/F_q}(\Phi_{p^n}(\zeta^{-j_k}x))=\frac{\Psi_{\tau_n(k)}(x^{p^n})}{\Psi_{\tau_{n-1}(k)}(x^{p^{n-1}})}\in F_q[x] \qquad n\geqslant 1 \qquad (3)$$

Specially, $\Theta_1^{(k)}(x)=\Psi_k(x)$.

Proof Since u is a prime, a root ζ^{j_k} of $\Psi_k(x)$ is a u-th primitive root of unity. Hence $F_q(\zeta^{j_k})=F_{q^m}=F_q(\zeta)$ and $\deg\Psi_k(x)=m$ for $k=1,2,\ldots,t$. Since the Galois group $\mathrm{Gal}(F_{q^m}/F_q)=(\sigma)$ is a cyclic group of order m and $\sigma(\zeta)=\zeta^q$, m is the order of q modulo u and $t=(u-1)/m$.

Let ζ^{j_k} be a root of $\Psi_k(x)$ for $k=1,2,\ldots,t$ and $\mathrm{Gal}(F_{q^m}/F_q)=(\sigma)$, then $\{1,\sigma^i(\zeta^{1_k})\mid i=1,2,\ldots,m;k=1,2,\ldots,t\}$ is the set of all roots of the u-th unity. By $\gcd(u,p)=1$, $\{1,\sigma^i(\zeta^{j_k})\mid i=1,2,\ldots,m;k=1,2,\ldots,t\}$ is also the set of all roots of the u-th unity. Hence for each j_k, there is a unique j_h such that $\{\sigma(\zeta^{j_kp^n}),\ldots,\sigma^m(\zeta^{j_kp^n})\}=\{\sigma(\zeta^{j_k}),\ldots,\sigma^m(\zeta^{j_k})\}$, which is equivalent to that $\zeta^{j_kp^n}$ is a root of $\Psi_h(x)$. Then $\tau_n(n\geqslant 1)$: $\{1,2,\ldots,t\}\to\{1,2,\ldots,t\}$, $k\to h$, is a permutation, where ζ^{j_k} is a root of $\Psi_k(x)$ and $\zeta^{j_kp^n}$ is a root of $\Psi_h(x)$. We have

$$\Psi_{\tau_n(k)}(x^{p^n})=\Psi_h(x^{p^n})=aN_{F_{q^n}/F_q}(x^{p^n}-\zeta^{j_kp^n})=N_{F_{q^n}/F_q}(1-(\zeta^{-j_k}x)^{p^n})$$

where $a=N_{F_{q^n}/F_q}(-\zeta^{-j_k})$, and

$$1-(\zeta^{-j_k}x)^{p^n}=(1-(\zeta^{-j_k}x)^{p^{n-1}})\Phi_{p^n}(\zeta^{-j_k}x)$$

Hence

$$\Theta_{p^n}^{(k)}(x)=N_{F_{q^n}/F_q}(\Phi_{p^n}(\zeta^{-j_k}x))=\frac{\Psi_{\tau_n(k)}(x^{p^n})}{\Psi_{\tau_{n-1}(k)}(x^{p^{n-1}})}\in F_q[x]$$

Let θ be a root of the irreducible polynomial $\Phi_{p^n}(\zeta^{-j_k}x)$ over F_{q^m}; i.e., θ is also a root of $\Theta_{p^n}^{(k)}(x)$. Then θ is a up^n-th primitive root of unity, and $K=F_q(\theta)=F_{q^m}(\theta)$. Since $[K:F_q]=[F_{q^m}(\theta):F_q]=[F_{q^m}(\theta):F_{q^m}][F_{q^m}:F_q]=m(p^n-p^{n-1})$ and $\deg\Theta_{p^n}^{(k)}(x)=m(p^n-p^{n-1})$, $\Theta_{p^n}^{(k)}(x)$ is irreducible over F_q for $k=1,2,\ldots,t$.

In Lemma 2, suppose that $\zeta^{j'}$ and $\zeta^{j''}$ are two roots of $\Psi_k(x)$, then there exist some $\sigma^i\in\mathrm{Gal}(F_{q^m}/F_q)$ such that $\sigma^i(\zeta^{j'})=\zeta^{j''}$. Hence $\sigma^i(s^{(j')})=s^{(j'')}$ and $\sigma^i(f_{s^{(j')}}(\zeta^{-j'}x))=f_{s^{(j'')}}(\zeta^{-j''}x)$. Take a root ζ^{j_k} of $\Psi_k(x)=0$ for $k=1,2,\ldots,t$, then $\{\zeta^0=1,\sigma^i(\zeta^{j_k})\mid i=1,2,\ldots,m;k=1,2,\ldots,t\}$ is the set of all roots of x^u-1 and $tm=u-1$. By Lemmas 1, 2 and 3, we have the following result.

Theorem 1 Let p, q, u and m be defined as above. Let ζ^{j_k} be a root of $\Psi_k(x)=0$ for $k=1,2,\ldots,t(=(u-1)/m)$, where $\Psi_k(x)$ is defined as Eq. (2). Let s be an $N(=up^n)$-periodic sequence over F_q. We have p^n-periodic sequences $s^{(0)}, s^{(j_1)},\ldots,s^{(j_t)}$ over F_{q^m} as Lemma 2.

1) Then

$$f_s(x) = f_{s^{(0)}}(x) g_{s^{(j_1)}}(x) \ldots g_{s^{(j_t)}}(x)$$
$$c(s) = c(s^{(0)}) + m(c(s^{(j_1)}) + \ldots + c(s^{(j_t)}))$$

where $g_{s^{(j_k)}}(x) = N_{F_{q^m}/F_q}(f_{s^{(j_k)}}(\zeta^{-j_k}x)) \in F_q[x]$ for $k = 1, 2, \ldots, t$.

2) For each $g_{s^{(j_k)}}(x)$, if $A_1^{(j_k)} = A_2^{(j_k)} = \ldots = A_p^{(j_k)}$, then

$$g_{s^{(j_k)}}(x) = N_{F_{q^n}/F_q}(f_{a^{(j_k)}}(\zeta^{-j_k}x))$$

Otherwise,

$$g_{s^{(j_k)}}(x) = N_{F_{q^n}/F_q}(f_{b^{(j_k)}}(\zeta^{-j_k}x)) \Theta_{p^n}^{(k)}(x)$$

where p^{n-1}-periodic sequences $a^{(j_k)}$ and $b^{(j_k)}$ are defined as Lemma 2 and $\Theta_{p^n}^{(k)}(x)$ is defined as Eq. (3).

Remark In order to compute the minimal polynomial of a up^n-periodic sequence, by the method of Ref. [3] we need to compute the minimal polynomials of u number of p^n-periodic sequences over F_{q^m}. By the method of Theorem 4 we only need to calculate the minimal polynomials of $(u-1)/m+1$ number of p^n-periodic sequences over F_{q^m}. Specially, if $m = u-1$, we only need to compute the minimal polynomials of two p^n-periodic sequences over F_{q^m}.

2 Application

In this section, we use Theorem 4 to give a fast algorithm for computing the linear complexities of a sequence with period $N = up^n$ over F_q.

Let p, q, u and m be defined as above, and let

$$1 - x^u = (1-x)\Psi_1(x) \ldots \Psi_t(x)$$

where $\Psi_k(x)$ is irreducible over F_q for $k = 1, 2, \ldots, t$ ($t = (u-1)/m$). Take a root $\zeta^{j_k} \in F_{q^m}$ of $\Psi_k(x)$ for $k = 1, 2, \ldots, t$, and let $j_0 = 0$.

We need to store $t+1$ elements $\zeta^{(j_0)}$, $\zeta^{(j_1)}$, …, $\zeta^{(j_t)}$ and $\Theta_{p^n}^{(0)}(x) = \Phi_{p^n}(x)$, $\Theta_{p^n}^{(1)}(x)$, …, $\Theta_{p^n}^{(t)}(x)$, which are defined as Eq. (3).

Algorithm 1

Input: An N-periodic ($N = up^n$) sequence $s = (s_0, s_1, \ldots)$ over F_q.

Output: The linear complexity $c(s)$ and $f_s(x)$.

Perform the reduction of Lemma 2 and we obtain p^n-periodic sequences $s^{(j_0)}$, $s^{(j_1)}$, …, $s^{(j_t)}$.

For the p^n-periodic sequences $s^{(j_0)}$, $s^{(j_1)}$, …, $s^{(j_t)}$, perform the Xiao-Wei-Lam-Imamura algorithm XWLI, the outputs are the linear complexities $c(s^{(j_0)})$, $c(s^{(j_1)})$, …, $c(s^{(j_t)})$ and the minimal connection polynomials $g_{s^{(0)}}(x) = f_{s^{(0)}}(x)$, $g_{s^{(j_1)}}(x)$, …, $g_{s^{(j_t)}}(x)$.

Initial values: $k \leftarrow j_k$, $a \leftarrow s^{(j_k)}$, $1 \leftarrow p^n$, $c \leftarrow 0$, $g \leftarrow 1$.

1) If $l = 1$, go to 2); otherwise $l \leftarrow l/p$ and go to step 3).

2) If $a = (0)$, stop; otherwise $c \leftarrow c+1$, $g \leftarrow g\Theta_1^{(k)}(x)$, stop.

3) If $A_1 = A_2 = \ldots = A_p$, $a \leftarrow A_1$, go to 1); otherwise $b \leftarrow A_1 + A_2 + \ldots + A_p$, $c \leftarrow c + (p-1)l$, $g \leftarrow g\Theta_{pl}^{(k)}(x)$ and go to step 4).

4) If $b = (0, 0, \ldots, 0)$, then stop; otherwise $a \leftarrow b$, go to step 1).

The final output c and g of the XWLI is the linear complexity of $c(s^{(j_k)})$ and $g_{s^{(j_k)}}(x) = g$ of the p^n-periodic sequences $s^{(j_k)}$ over F_{q^m}.

Finally we obtain the linear complexity of $c(s) = c(s^{(0)}) + m\sum_{k=1}^{t} c(s^{(j_k)})$ and the minimal connection polynomial $f_s(x) = \prod_{k=0}^{t} g_{s^{(j_k)}}(x)$.

Example 1 $q = 2$, $u = 7$, $p = 5$, 3 is the order of 2 modulo 7, 2 is a primitive root modulo 25, and $\gcd(3, 5(5-1)) = 1$.

$1 - x^7 = (1-x)(1+x+x^3)(1+x^2+x^3)$ over F_2. Let ζ be a root of $\Psi_1(x) = 1 + x + x^3$, then ζ, ζ^2, ζ^4 are roots of $\Psi_1(x)$ and ζ^3, ζ^5, ζ^6 are roots of $\Psi_2(x) = 1 + x^2 + x^3$. In Lemma 3, $t = 2$, $j_1 = 1$, $j_2 = 3$. Since $5^3 \equiv 6 \bmod 7$ and $5^2 \equiv 4 \bmod 7$, $\tau_3(1) = 2$ and $\tau_2(1) = 1$. Hence $N_{F_{2^3}/F_2}(\Phi_{5^3}(\zeta^{-1}x)) = \Psi_2(x^{5^3})/\Psi_1(x^{5^2})$.

Since $\zeta^3 = 1 + \zeta$, $\zeta^4 = (1+\zeta)\zeta = \zeta + \zeta^2$, $\zeta^5 = (1+\zeta)\zeta^2 = \zeta^2 + \zeta + 1$, $\zeta^6 = (1+\zeta)^2 = 1 + \zeta^2$, we have a formula: $a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 + a_5\zeta^5 + a_6\zeta^6 = (a_0 + a_3 + a_5 + a_6) + (a_1 + a_3 + a_4 + a_5)\zeta + (a_2 + a_4 + a_5 + a_6)\zeta^2$ over $F_2(\zeta)$.

Let $s = (s_0, s_1, s_2, \ldots)$ be a sequence with period $N = 5 \times 7$ over F_2. Let $s^{(0)}$, $s^{(1)}$, $s^{(3)}$ be sequences from Lemma 2. For $s^{(0)}$,

$$\begin{aligned}
s_0^{(0)} &= s_0 + s_p + s_{2p} + s_{3p} + s_{4p} + s_{5p} + s_{6p} \\
s_1^{(0)} &= s_1 + s_{p+1} + s_{2p+1} + s_{3p+1} + s_{4p+1} + s_{5p+1} + s_{6p+1} \\
s_2^{(0)} &= s_2 + s_{p+2} + s_{2p+2} + s_{3p+2} + s_{4p+2} + s_{5p+2} + s_{6p+2} \\
s_3^{(0)} &= s_3 + s_{p+3} + s_{2p+3} + s_{3p+3} + s_{4p+3} + s_{5p+3} + s_{6p+3} \\
s_4^{(0)} &= s_4 + s_{p+4} + s_{2p+4} + s_{3p+4} + s_{4p+4} + s_{5p+4} + s_{6p+4}
\end{aligned}$$

For $s^{(1)}$, by $(0, p, 2p, 3p, 4p, 5p, 6p) \equiv (0, 5, 3, 1, 6, 4, 2) \bmod 7$,

$$\begin{aligned}
s_0^{(1)} &= (s_0 + s_p + s_{2p} + s_{4p}) + (s_p + s_{2p} + s_{3p} + s_{5p})\zeta + (s_p + s_{4p} + s_{5p} + s_{6p})\zeta^2 \\
s_1^{(1)} &= (s_{p+1} + s_{4p+1} + s_{5p+1} + s_{6p+1}) + (s_1 + s_{2p+1} + s_{5p+1} + s_{6p+1})\zeta + (s_{p+1} + s_{2p+1} + s_{3p+1} + s_{5p+1})\zeta^2 \\
s_2^{(1)} &= (s_{p+2} + s_{2p+2} + s_{3p+2} + s_{5p+2}) + (s_{2p+2} + s_{3p+2} + s_{4p+2} + s_{6p+2})\zeta + (s_2 + s_{2p+2} + s_{5p+2} + s_{6p+2})\zeta^2 \\
s_3^{(1)} &= (s_3 + s_{2p+3} + s_{5p+3} + s_{6p+3}) + (s_3 + s_{p+3} + s_{3p+3} + s_{6p+3})\zeta + (s_{3p+3} + s_{2p+3} + s_{4p+3} + s_{6p+3})\zeta^2 \\
s_4^{(1)} &= (s_{2p+4} + s_{3p+4} + s_{4p+4} + s_{6p+4}) + (s_4 + s_{3p+4} + s_{4p+4} + s_{5p+4})\zeta + (s_4 + s_{p+4} + s_{3p+4} + s_{6p+4})\zeta^2
\end{aligned}$$

For $s^{(3)}$, by $(0, 3p, 6p, 9p, 12p, 15p, 18p) \equiv (0, 1, 2, 3, 4, 5, 6) \bmod 7$,

$$\begin{aligned}
s_0^{(3)} &= (s_0 + s_{3p} + s_{5p} + s_{6p}) + (s_p + s_{3p} + s_{4p} + s_{5p})\zeta + (s_{2p} + s_{4p} + s_{5p} + s_{6p})\zeta^2 \\
s_1^{(3)} &= (s_1 + s_{2p+1} + s_{3p+1} + s_{4p+1}) + (s_1 + s_{p+1} + s_{2p+1} + s_{5p+1})\zeta + (s_{p+1} + s_{2p+1} + s_{3p+1} + s_{6p+1})\zeta^2 \\
s_2^{(3)} &= (s_2 + s_{p+2} + s_{4p+2} + s_{6p+2}) + (s_{2p+2} + s_{4p+2} + s_{5p+2} + s_{6p+2})\zeta + (s_2 + s_{3p+2} + s_{5p+2} + s_{6p+2})\zeta^2
\end{aligned}$$

$$s_3^{(3)} = (s_{P+3} + s_{3p+3} + s_{4p+3} + s_{5p+3}) + (s_{p+3} + s_{2p+3} + s_{3p+3} + s_{6p+3})\zeta + (s_3 + s_{2p+3} + s_{3p+3} + s_{4p+3})\zeta^2$$

$$s_4^{(3)} = (s_4 + s_{p+4} + s_{2p+4} + s_{5p+4}) + (s_4 + s_{3p+4} + s_{5p+4} + s_{6p+4})\zeta + (s_4 + s_{p+4} + s_{4p+4} + s_{6p+4})\zeta^2$$

Let s be a sequence with the first period (11001; 11110; 00110; 10001; 11100; 01111; 00010). We also write it as a 7×5 matrix:

$$S^N = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Then $s^{(0)}$ has the first sequence $(0, 0, 0, 0, 1)$. By Lemma 1, $f_{s^{(0)}}(x) = 1 - x^5$. $s^{(1)}$ has the first sequence $(s_0^{(1)}, s_1^{(1)}, s_2^{(1)}, s_3^{(1)}, s_4^{(1)}) = (1, 1, 1, 1, 1 + \zeta)$, $g_{s^{(1)}}(x) = N_{F_2/F_1}(f_b(\zeta^{-1}x))\Theta_p^{(1)}(x) = \Psi_1(x)\Theta_p^{(1)}(x) = \Psi_2(x^5)$, where $\tau_1(1) = 2, \tau_0(1) = 1$ and the sequence b is a 1-periodic sequence with the first period $(1 + \zeta)$. $s^{(3)}$ has the first sequence $(s_0^{(3)}, s_1^{(3)}, s_2^{(3)}, s_3^{(3)}, s_4^{(3)}) = (\zeta + \zeta^2, \zeta + \zeta^2, \zeta + \zeta^2, \zeta + \zeta^2, \zeta + \zeta^2)$.

$g_{s^{(3)}}(x) = N_{F_2/F_2}(f_a(\zeta^{-3}x)) = \Psi_2(x)$, where a is a 1-periodic sequence with the first period $(\zeta + \zeta^2)$. Hence $f_s(x) = (1 - x^5)\Psi_2(x)\Psi_2(x^5)$ and $c(s) = 5 + 3 + 3 \cdot 5 = 23$.

We can use the algorithm to compute the minimal polynomial and linear complexity of a sequence with period $N = 7 \cdot 5^n$ over F_2.

3 Conclusion

In Ref. [3], we have known an algorithm for determining the minimal polynomial and linear complexity of a up^n-periodic sequence over F_{q^m} with $u \mid q^m - 1$. In fact, if $\Phi_{p^n}(x)$ is reducible over F_{q^m}, then we cannot use the XWLI algorithm[10]. This paper is supplementary to Ref. [3]. In this paper, we assume that p, q and u are distinct primes; q is a primitive root modulo p^2; m is the order of q modulo u; and $\gcd(m, p(p-1)) = 1$. Under the assumption, we can use the algorithm in Ref. [3] to determine the minimal polynomial and linear complexity of a up^n-periodic sequence over F_{q^m} with time complexity $O(N)$. Moreover, we give a fast algorithm to determine the minimal polynomial and linear complexity of a up^n-periodic sequence over F_q, which combines the algorithms of Ref. [3] and Ref. [10]. We can use the algorithm to determine the minimal polynomial and linear complexity of a sequence with period $N = 7 \cdot 5^n$ over F_2.

References

[1] Blackburn S R. A generalization of the discrete Fourier transform: determining the minimal polynomial of a period sequence[J]. *IEEE Trans Inf Theory*, 1994, **40**(5): 1702 - 1704.

[2] Chen H. Fast algorithms for determining the linear complexity of sequences over GF(p^m) with period $2^t n$[J]. *IEEE Trans Inf Theory*, 2005, **51**(5): 1854 - 1856.

[3] Chen H. Reducing the computation of linear complexities of periodic sequences over GF(p^m)[J]. *IEEE Trans Inf Theory*, 2006, **52**(12): 5537 - 5539.

[4] Ding C. A fast algorithm for the determination of linear complexity of sequences over GF(p^m) with period p^n[C]//*Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 1991: 141 - 144.

[5] Ding C, Xiao G, Shan W. *The stability theory of stream ciphers* (*Lecture Notes in Computer Science* 561)[M]. Berlin: Springer-Verlag, 1991.

[6] Games R A, Chan A H. A fast algorithm for determining the complexity of a binary sequence with period 2^n[J]. *IEEE Trans Inf Theory*, 1983, **29**(1): 144 - 146.

[7] Lidl R, Niederreiter H. *Finite fields*[M]. Addison-Wesley Publishing Company, 1983.

[8] Massey J L. Shift register synthesis and BCH decoding[J]. *IEEE Trans Inf Theory*, 1969, **15**(1): 122 - 127.

[9] Wei S, Xiao G, Chen Z. A fast algorithm for determining the minimal polynomial of a sequence with $2p^n$ over GF(q)[J]. *IEEE Trans Inf Theory*, 2002, **48**(10): 2754 - 2758.

[10] Xiao G, Wei S, Lam K Y, et al. A fast algorithm for determining the linear complexity of a sequence with p^n over GF(q)[J]. *IEEE Trans Inf Theory*, 2000, **46**(6): 2203 - 2206.

决定周期为 up^n 序列的极小多项式的快速算法

胡卫群[1]　　岳　勤[2]

([1] 南京林业大学理学院,南京 210037)

([2] 南京航空航天大学理学院,南京 210016)

摘要:给出了一个快速算法决定有限域 F_q 上周期为 up^n 序列的极小多项式. 设 p, q, u 为不同素数,q 为模 p^2 的本原根,m 为最小正整数使得 $q^m \equiv 1 \bmod u$ 和 $\gcd(m, p(p-1)) = 1$. 利用一个算法把有限域 F_q 上周期为 up^n 序列化为几个有限域 $F_q(\zeta)$ 上周期为 p^n 序列,其中 ζ 为一个 u 次本原单位根,从而利用肖国正等的算法得到每个周期为 p^n 序列的极小多项式.

关键词:极小多项式;线性复杂度;周期序列

中图分类号:O236.2