F_q 上具有极大 1-error 线性复杂度的周期序列*

胡红钢[1,2+], 冯登国[1]

[1](信息安全国家重点实验室(中国科学院研究生院),北京 100049)

[2](中国科学院 电子学研究所,北京 100080)

Periodic Sequences with very Large 1-Error Linear Complexity over F_q

HU Hong-Gang[1,2+], FENG Deng-Guo[1]

[1](State Key Laboratory of Information Security (Graduate School of the Chinese Academy of Sciences), Beijing 100049, China)

[2](Institute of Electronics, The Chinese Academy of Sciences, Beijing 100080, China)

+ Corresponding author: Phn: +86-10-88256432 ext 64, E-mail: hg_hu@163.net, http://home.is.ac.cn

Received 2003-06-23; Accepted 2003-11-10

Hu HG, Feng DG. Periodic sequences with very large 1-error linear complexity over F_q. *Journal of Software*, 2005,16(5):940−945. DOI: 10.1360/jos160940

Abstract: Linear complexity is an important design index for assessing the cryptographic strength of a sequence. Pseudorandom sequences with large linear complexity and large k-error linear complexity is a hot topic in cryptography and communications. Niederreiter found many such periodic sequences over F_q firstly. In this paper, the authors construct some periodic sequences over F_q with very large 1-error linear complexity by the GDFT of a periodic sequence. The result is much better than the known ones.

Key words: periodic sequence; GDFT; linear complexity; 1-error linear complexity

摘 要: 线性复杂度是衡量序列密码学强度的重要指标,设计具有大的线性复杂度和 k-error 线性复杂度的序列是密码学和通信中的热点问题.Niederreiter 首次发现了 F_q 上许多满足这个要求的周期序列.通过序列的广义离散傅立叶变换构造了一些 F_q 上具有极大 1-error 线性复杂度的周期序列,这些结果远远优于已知的结果.

关键词: 周期序列;广义离散傅立叶变换;线性复杂度;1-error 线性复杂度

中图法分类号: TP309 **文献标识码**: A

Pseudorandom sequences have been used widely in communications and cryptography. These sequences are required to have certain properties: long period, two-level autocorrelation, large linear complexity and etc. Let S be a sequence of linear complexity L over F_q, where L is the least order of a linear recurrence relation satisfied by S,

* Supported by the National Nature Science Foundation under Grant No.60273027 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the National Science Fund for Distinguished Young Scholars under Grant No.60025205 (国家杰出青年科学基金)

HU Hong-Gang was born in 1978. He is a Ph.D. candidate at the State Key Laboratory of Information Security (Graduate School of the Chinese Academy of Sciences). His current research areas are cryptography and information security. **FENG Deng-Guo** was born in 1965. He is a professor and doctoral supervisor at the State Key Laboratory of Information Security (Graduate School of the Chinese Academy of Sciences). His research areas are cryptography and information security.

the well known B-M algorithm needs only 2L elements to determine the LFSR which can generate S[1]. Hence, the linear complexity is an important index for assessing the cryptographic strength of a pseudorandom sequence.

Ding and Stamp independently proposed the new concept of k-error linear complexity which is the generalization of linear complexity[2,3]. A sequence with large k-error linear complexity not only has a large linear complexity, but also has the feature that altering up to k terms should not cause a significant decrease of the linear complexity. Much work has been done on this topic[2−9]. In the next section, we will give the formal definition of k-error linear complexity.

Kolokotronis, Rizomiliotis and Kalouptsidis discussed the determination of the minimum linear complexity sequence which is got from a given binary sequence with period 2^n−1 by at most one symbol substitution[5]. They presented three methods for this problem: the sequential division method, the congruential equations, and the phase synchronization method. However they only gave some guidelines on sequence design. Niederreiter proved the existence of periodic sequences which have large k-error linear complexity when k over a finite field is small[6], but there are too many constraints on the period N.

In this paper, we construct some periodic sequences with large linear complexity and large 1-error linear complexity over F_q by the generalized discrete Fourier transform(GDFT) of a periodic sequence. This result is better than that of Ref.[6] and extends the result of Ref.[5]. In Section 2, we briefly introduce some notations. In Section 3, we drive the main result. Finally, section 4 contains the conclusions.

1 Notations and Preparations

Let S=s_0,s_1,s_2,… be a sequence over a finite field F_q. If S_i=S_{i+N} for all i≥0, we call it N-periodic. Because S is completely determined by its first N terms, we can describe S by $S=(s_0,s_1,s_2,...,s_{N-1})^\infty$. The polynomail $S^N(x)$ is defined as $S^N(x)=s_0+s_1x+s_2x^2+...+s_{N-1}x^{N-1}$.

Firstly, we will give the formal definition of k-error linear complexity of periodic sequence below.

Definition 1. Let $S=(s_0,s_1,s_2,...,s_{N-1})^\infty$ be an N-periodic sequence over F_q and k be an integer with $1\le k\le N$, then the k-weight-error linear complexity $C_{N,k}(S)$ of S is $\min_T L(T)$, where the minimum is extended over all N-periodic sequences $T=(t_0,t_1,t_2,...,t_{N-1})^\infty$ over F_q for which the Hamming distance of $(s_0,s_1,s_2,...,s_{N-1})$ and $(t_0,t_1,t_2,...,t_{N-1})$ is exactly k.

Definition 2. Let $S=(s_0,s_1,s_2,...,s_{N-1})^\infty$ be an N-periodic sequence over F_q and k be an integer with $1\le k\le N$, then the k-error linear complexity $L_{N,k}(S)$ is defined as $\min_{0\le k'\le k} C_{N,k'}(S)$.

The definitions above are also contained in Ref.[6].

Let $F[x]$ denotes the ring of polynomials with coefficients in a field F, and $g(x)=\sum_i a_i x^i\in F[x]$. For any integer $t\ge 0$, the t th Hasse derivative of $g(x)$ is defined as $g^{[t]}(x)=\sum_i \binom{i}{t} a_i x^{i-t}$. It is easy to verify that $g^{(t)}(x)=t!g^{[t]}(x)$, where $g^{(t)}(x)$ is the t th usual formal derivative of $g(x)$. When t=1, $g^{(1)}(x)=g^{[1]}(x)$.

From now on, we denote p as the characteristic of F_q. In accordance with Ref.[10], the authors of Ref.[8] give the following definition.

Definition 3[8]. The GDFT of the $S^N=(s_0,s_1,...,s_{N-1})\in F_q^N, N=p^v n, \gcd(n,p)=1$ is defined to be the $p^v\times n$ matrix of the Hasse derivatives, where α is any primitive nth root of unity in some extension field of F_q and $S^N(x)=s_0+s_1x+s_2x^2+...+s_{N-1}x^{N-1}$.

$$S^{p^v\times n}=GDFT(S^N)=\begin{pmatrix} S^N(1) & S^N(\alpha) & \dots & S^N(\alpha^{n-1}) \\ (S^N)^{[1]}(1) & (S^N)^{[1]}(\alpha) & \dots & (S^N)^{[1]}(\alpha^{n-1}) \\ \dots & \dots & \dots & \dots \\ (S^N)^{[p^v-1]}(1) & (S^N)^{[p^v-1]}(\alpha) & \dots & (S^N)^{[p^v-1]}(\alpha^{n-1}) \end{pmatrix}.$$

The GDFT of a periodic sequence over F_q is indeed an invertible transformation, which is shown in Ref.[10]. If $\gcd(N,p)=1$, then α is a primitive Nth root of unity and the GDFT of an N-tuple reduces to the discrete Fouier transform (DFT) of the same N-tuple.

The following lemma is the basis for our result in this paper.

Lemma 1. Let $E_k=(e_0,e_1,...,e_{N-1})$ be a N-length vector of weight 1 over F_q, the single nonzero one be the kth digit, where $k\in Z_N$, then $E_k(x)=e_kx^k$ and

$$GDFT(E_k)=\begin{pmatrix} e_k & e_k\alpha^k & \dots & e_k\alpha^{(n-1)k} \\ \binom{k}{1}e_k & \binom{k}{1}e_k\alpha^{(k-1)} & \dots & \binom{k}{1}e_k\alpha^{(n-1)(k-1)} \\ \dots & \dots & \dots & \dots \\ \binom{k}{p^v-1}e_k & \binom{k}{p^v-1}e_k\alpha^{(k-p^v+1)} & \dots & \binom{k}{p^v-1}e_k\alpha^{(n-1)(k-p^v+1)} \end{pmatrix}$$

where α is any primitive nth root of unity and $\binom{i}{j}=0$ if $i<j$.

Now we need the following useful definition.

Definition 4 [8]. The Günther weight of a matrix is the number of its entries that are nonzero or that lie below a nonzero entry.

The proposition below states the important relationship between the linear complexity of the N-periodic sequence $S=(s_0,s_1,s_2,...,s_{N-1})^\infty$ and the (G)DFT of the corresponding N-tuple $S^N=(s_0,s_1,...,s_{N-1})$.

Proposition 1. (Günther-Blahut Theorem) [8]. The linear complexity of the N-periodic sequence $S=(s_0,s_1,s_2,...,s_{N-1})^\infty$ over F_q of the characteristic p, where $N=p^vn$ and $\gcd(n,p)=1$, is equal to the Günther weight of the GDFT of the N-tuple $S^N=(s_0,s_1,...,s_{N-1})$.

2 Main Results

We have the following lemma from Ref.[8], and it will give us more information about the structure of the GDFT of an N-tuple. Note that cyclotomic cosets will be considered relative to powers of q in the following.

Lemma 2 [8]. For an integer $0\le j\le n-1$, let the integer $0\le k\le n-1$ be an element of the cyclotomic coset C_j of j modulo n, i.e., $k\equiv jq^r \bmod n$ for some integer $r\ge 0$. Let $|C_j|=l_j$, then for any $0\le t\le p^v-1$, we have $(S^N)^{[t]}(\alpha^j)\in F_{q^{l_j}}$ and $(S^N)^{[t]}(\alpha^k)=((S^N)^{[t]}(\alpha^j))^{q^r}$.

Let the sets $C_1,C_2,...,C_h$ be the different cyclotomic cosets modulo n (relative to powers of q), where $C_1=\{0\}$, and $|C_j|=l_j, 1\le j\le h$, $l_2\ge l_3\ge ...\ge l_h$. By Lemma 2, a GDFT is uniquely determined by h p^v-dimensional column vectors, one vector for each cyclotomic coset. The components of the column vector corresponding to the cyclotomic coset C_j are in $F_{q^{l_j}}$. Hence, any GDFT uniquely corresponds to a $p^v\times h$ matrix M, where the entries in the ith column of M are in $F_{q^{l_i}}$. The number of different matrices of this form is $(q^{l_{j1}})^{p^v}(q^{l_{j2}})^{p^v}...(q^{l_{jh}})^{p^v}=q^{np^v}=q^N$ which is just the number of all N-periodic sequence over F_q. So we have the following important lemma.

Lemma 3 [8]. There is a bijection from the set of all N-periodic sequence over F_q onto the set of all matrices in GDFT form.

Suppose $S=(s_0,s_1,s_2,...,s_{N-1})^{\infty}$ is a N-periodic sequence over F_q of the characteristic p, $E_k=(0,0,...,0,e_k,0,...,0,0)^{\infty}$ is another N-periodic sequence over F_q, where $0\le k\le N-1$, then $C_{N,1}(S)=\min\limits_{e_k\in F_q^*,0\le k\le N-1} L(S+E_k)$ $=\min\limits_{e_k\in F_q^*,0\le k\le N-1} W(GDFT(S+E_k))=\min\limits_{e_k\in F_q^*,0\le k\le N-1} W(GDFT(S)+GDFT(E_k))$, where $W(\cdot)$ denote the Günther weight of a matrix. If $S^N(1)\ne 0$, then it is obvious that $\min\limits_{e_k\in F_q^*,0\le k\le N-1} W(GDFT(S)+GDFT(E_k))\le N-1$. This is just the Corollary 1 of Ref.[6].

Theorem 1. Let $N=np^v,\gcd(n,p)=1,v\ge 1$, and the sets $C_1,C_2,...,C_h$ be the cyclotomic cosets module n (relative to powers of q), where $C_1=\{0\}$, and $|C_j|=l_j,l_2\ge l_3\ge ...\ge l_h$, $1\le j\le h$, if $q^{l_h}>p$, then there exists a N-periodic sequence S over F_q of the characteristic p such that: $L(S)=N-1,C_{N,1}(S)\ge N+1-n$. Furthermore, the number of such sequences is at least $q^{n(p^v-2)}\prod\limits_{j=2}^{h}(q^{l_j}-p)\prod\limits_{j=1}^{h}(q^{l_j}-1)$.

Proof. Firstly, according to lemma 3, we can let $S^N(1)=0$, $(S^N)^{[i]}(1)$ be arbitrary, $1\le i\le p^v-1$, but $(S^N)^{[1]}(1)\ne 0$. Secondly, for $\forall 1\le i\le n-1$ and $\forall S^N(\alpha^i)\in F_{q^{l_{j_0}}}^*, i\in C_{j_0}, 2\le j_0\le h$, we can select $(S^N)^{[1]}(\alpha^i)\in F_{q^{l_{j_0}}}-\{k\alpha^{-i}S^N(\alpha^i)\mid k\in Z_N\}$ since $q^{l_{j_0}}\ge q^{l_h}>p$. So $S^N[\alpha^i]+e_k\alpha^{ik}=0$, and $(S^N)^{[1]}[\alpha^i]+ke_k\alpha^{i(k-1)}=0$ will not be true simultaneously. Thirdly, let $(S^N)^{[t]}(\alpha^i)$ be arbitrary, where $2\le t\le p^v-1, 1\le i\le n-1$. Therefore, $\min\limits_{e_k\in F_q^*,0\le k\le N-1} W(GDFT(S+E_k))\ge N+1-n$, where E_k is the same as above. So $L(S)=N-1$, and $C_{N,1}(S)\ge N+1-n$ by Proposition 1.

By Lemma 3, the number of such sequences is at least $(q^{l_1})^{p^v-2}(q^{l_2})^{p^v-2}...(q^{l_h})^{p^v-2}(q^{l_2}-p)...(q^{l_h}-p)(q^{l_1}-1)(q^{l_2}-1)...(q^{l_h}-1)=q^{n(p^v-2)}\prod\limits_{j=2}^{h}(q^{l_j}-p)\prod\limits_{j=1}^{h}(q^{l_j}-1)$.

Remark 1.1. The condition $q^{l_h}>p$ is loose: $l_h\ge 1$ when $q>p$; $l_h\ge 2$ when $q=p$. The condition in Ref.[6] is $N(q-1)+1<q^{l_h}\Leftrightarrow N<(q^{l_h}-1)/(q-1)$. It is stricter.

Remark 1.2. If $N=p^v,v\ge 1$, the result of theorem 1 of Ref.[6] is trivial, but our result is nontrivial.

Lemma 4. $n>2,\gcd(n,2)=1$, let l be the order of 2 module n and α be any primitive n th root of unity, then for any $A\in F_{2^l}$ and $1\le i\le n-1,\gcd(i,n)=1$, there exists at most one $1\le k\le n-1$, such that $\alpha^{ik}+A=0$.

Proof. If there exists $1\le k_1<k_2\le n-1$, such that $\alpha^{ik_1}+A=0$ and $\alpha^{ik_2}+A=0$, then $\alpha^{ik_1}=\alpha^{ik_2}\Leftrightarrow\alpha^{i(k_2-k_1)}=1\Leftrightarrow n\mid i(k_2-k_1)\Leftrightarrow n\mid(k_1-k_2)$ since $\gcd(i,n)=1$, we have $k_1=k_2$. But it is a contradiction.

Theorem 2. If q=2,let $N=2^vn,\gcd(n,2)=1,n>2,v\ge 1$, and the sets $C_1,C_2,...,C_h$ be the cyclotomic cosets module n (relative to powers of 2), where $C_1=\{0\}$, and $|C_j|=l_j,l_2\ge l_3\ge ...\ge l_h,1\le j\le h$, if $l_h\ge 2$, then there exists a N-periodic binary sequence S over F_2 such that: $L(S)=N-1,C_{N,1}(S)\ge N+1-n+\phi(n)-l_2$, where $\phi(\cdot)$ is the Euler function. Furthermore, the number of such sequences is at least $2^{n(2^v-2)}\prod\limits_{j=2}^{t+1}(2^{l_j}-2)\prod\limits_{j=1}^{t}(n-j)\prod\limits_{j=t+2}^{h}(2^{l_j}-1)$, where $t=\phi(n)/l_2$.

Proof. Let $t=\phi(n)/l_2$, for $2\le j\le 1+t$, i_j is the coset leader of C_j, we can suppose $\gcd(n,i_j)=1,2\le j\le 1+t$. Let $S^N(\alpha^{i_2})=\alpha^{i_2k_2},1\le k_2\le n-1$. For $3\le j\le 1+t$, let $S^N(\alpha^{i_j})=\alpha^{i_jk_j},1\le k_j\le n-1$ and $k_j\ne k_{j'}$,

$2 \le j' < j$. We can select $(S^N)^{[1]}(\alpha^{i_j}) \in F_{2^{l_j}} - \{k\alpha^{-i_j} S^N(\alpha^{i_j}) \mid k \in Z_N\}, 2 \le j \le 1+t$ since $l_h \ge 2$. The remaining part of this proof is the same as Theorem 1. Then $L(S) = N-1, C_{N,1}(S) \ge N+1-n+\phi(n)-l_2$ by Lemma 4 and Proposition 1.

The number of such sequence is at least $(2^{l_{j_1}})^{2^{v-2}}(2^{l_{j_2}})^{2^{v-2}}...(2^{l_{j_h}})^{2^{v-2}}(2^{l_2}-2)...(2^{l_{j_h}}-2)(n-1)...(n-t)(2^{l_{t+2}}-1)...(2^{l_h}-1)$ $= 2^{n(2^{v-2})}\prod_{j=2}^{t+1}(2^{l_j}-2)\prod_{j=1}^{t}(n-j)\prod_{j=t+2}^{h}(2^{l_j}-1)$.

Remark 2.1. If n is prime and the order of 2 modulo n is $\phi(n)=n-1$, then theorem 2 is trivial. At that time, h=2, $l_2 = n-1, C_1 = \{0\}, C_2 = \{1,2,...,n-1\}$.

Remark 2.2. If n is prime and the order of 2 modulo n isn't $\phi(n) = n-1$, then l_2 is the order of 2 modulo n, $h = t$, and $C_{N,1}(S) \ge N - l_2$.

Theorem 3. Let $N = np^v, \gcd(n, p) = 1, v \ge 0$, and the sets $C_1, C_2, ..., C_h$ be the cyclotomic cosets module n (relative to powers of q), where $C_1 = \{0\}$, and $|C_j| = l_j, l_2 \ge l_3 \ge ... \ge l_h, 1 \le j \le h$, if $q^{l_h} - 1 > (q-1)n$, then there exists a N-periodic sequence S over F_q of the characteristic p such that: $L(S) = N-1, C_{N,1}(S) = N$. Furthermore, the number of such sequences is at least $(q-1)q^{n(p^v-1)-1}\prod_{j=2}^{h}(q^{l_j}-1-(q-1)n)$ when $v \ge 1$, and $\prod_{j=2}^{h}(q^{l_j}-1-(q-1)n)$ when $v = 0$.

Proof. Firstly, we can let $S^N(1) = 0$, $(S^N)^{[i]}(1)$ be arbitrary, $1 \le i \le p^v - 1$, but $(S^N)^{[1]}(1) \ne 0$, according to Lemma 3. Secondly, for $\forall 1 \le i \le n-1, i \in C_{j_0}, 2 \le j_0 \le h$, we can choose $S^N(\alpha^i) \in F^*_{q^{l_{j_0}}} - \{e_k\alpha^{ik} \mid e_k \in F_q^*, k \in Z_N\}$ since $q^{l_h} - 1 > (q-1)n$. Thirdly, let $(S^N)^{[t]}(\alpha^i)$ be arbitrary, where $1 \le t \le p^v - 1, 1 \le i \le n-1$. Therefore, $\min_{e_k \in F_q^*, 0 \le k \le N-1} W(GDFT(S+E_k)) = N$, where E_k is the same as above. So $L(S) = N-1, C_{N,1}(S) = N$ by Proposition 1.

The number of such sequences is at least $(q-1)(q^{l_1})^{p^{v-2}}(q^{l_2})^{p^{v-1}}...(q^{l_h})^{p^{v-1}}(q^{l_2}-1-(q-1)n)(q^{l_3}-1-(q-1)n)...$ $...(q^{l_h}-1-(q-1)n) = (q-1)q^{n(p^v-1)-1}\prod_{j=2}^{h}(q^{l_j}-1-(q-1)n)$ when $v \ge 1$, $(q^{l_2}-1-(q-1)n)(q^{l_3}-1-(q-1)n)...(q^{l_h}-1-(q-1)n)$ $= \prod_{j=2}^{h}(q^{l_j}-1-(q-1)n)$ when $v = 0$.

Remark 3.1. The condition in Ref.[6] is $N < (q^{l_h}-1)/(q-1)$, but our condition is $n < (q^{l_h}-1)/(q-1)$. So ours is better.

Remark 3.2. If $q = 2$ and $N = 2^k - 1$, there exists no such a binary sequence S of period N of Theorem 3 since $N \not< (q^{l_h}-1)/(q-1)$.

3 Conclusions

By the GDFT of a periodic sequence, we construct some periodic sequences over F_q with very large 1-error linear complexity in this paper. Our result has less constraints on the period N of the corresponding sequence, and can also extend the result of Ref.[5] (In Ref.[5], only binary sequence of period 2^n-1 is considered). We also show that (G)DFT of the periodic sequence is a powerful tool for sequence research. But how to get the sequence from its (G)DFT easily is another important problem. Furthermore, how to construct periodic sequences over F_q with large k-error linear complexity ($k \ge 2$) by (G)DFT is also an interesting problem.

References:

[1] Massey JL. Shift-Register synthesis and BCH decoding. IEEE Trans. on Information Theory, 1969,IT-15:122−127.

[2] Ding C, Xiao G, Shan W. The stability theory of stream ciphers. LNCS 561, Berlin: Springer-Verlag, 1991.

[3] Stamp M, Martin CF. An algorithm for the k -error linear complexity of binary sequences with period 2^n. IEEE Trans. on Information Theory, 1993,IT-39:1398−1401.

[4] Jiang S, Dai Z, Imamura K. Linear complexity of a sequence obtained from a periodic sequence by either substituting, inserting, or deleting *k* symbols within one period. IEEE Trans. on Information Theory, 2000,46:1174−1177.

[5] Kolokotronis N, Rizomiliotis P, Kalouptsidis N. Minimum linear span approximation of binary sequences. IEEE Trans. on Information Theory, 2002,IT-48:2758−2764.

[6] Niederreiter H. Periodic sequences with large k-error linear complexity. IEEE Trans. on Information Theory, 2003,IT-49:501−505.

[7] Dai Z, Imamura K. Linear complexity for one-symbol substitution of a periodic sequence over *GF*(*q*). IEEE Trans. on Information Theory, 1998,44:1328−1331.

[8] Meidl W, Niederreiter H. On the expected value of the linear complexity and the *k*-error linear complexity of periodic sequences. IEEE Trans. on Information Theory, 2002,IT-48:2817−2825.

[9] Meidl W, Niederreiter H. Linear complexity, *k*-error linear complexity, and the discrete Fourier transform. Journal of Complexity, 2002,18:87−103.

[10] Massey JL, Serconek S. Linear complexity of periodic sequences: A general theory. Advances in Cryptology-Crypto'96, LNCS 1109, Berlin: Springer-Verlag, 1996.358−371.

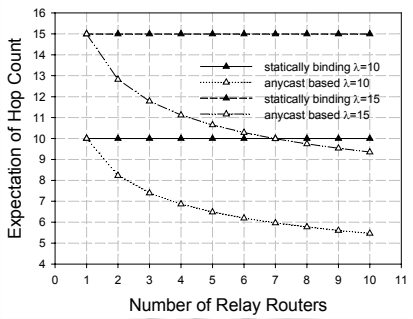

Fig.5 Expectation of Hopcount