Distribution of the Linear Complexities of Generalized Legendre Sequences*

WANG Ping, DAI Zong-duo

(*State Key Laboratory of Informational Security, Graduate School, The Chinese Academy of Sciences, Beijing* 100039, *China*)

E-mail: sh.p.wang@263.net

Received September 3, 2001; accepted April 9, 2002

Abstract: In the paper, an estimation of distribution of linear complexities of generalized Legendre sequences is made. It is discovered that most of the generalized Legendre sequences have large linear complexities. A way is proposed to find the generalized Legendre sequence of the large linear complexity.

Key words: linear complexity; generalized Legendre sequence

The design for the key sequences with perfect performance is always the hotspot in the digital communication and stream cipher stream cipher research. A good key sequence often has large linear complexity and strong pseudorandomness. Legendre sequences look random with respect to elementary statistical tests and also quite good from the linear complexity viewpoint[1,2]. About various statistical properties and linear complexities of the Legendre sequences, we refer to Refs.[3~6] for detail. Recently, the so-called generalized Legendre sequence $S_{\underline{b}}(p,R)$ is defined and its linear complexity is discussed in Ref.[7], where $R=r^t$ is a prime power, p is a prime such that $R|p$-1, and $\underline{b}$ is an arrangement of all elements in the finite field F_R of order R. In Ref.[7], the linear complexities of the sequences $S_{\underline{b}}(p,R)$ are determined for the cases when R=3 and 4, and some partial results for the cases when R=8 or an odd prime r.

We introduce some notations and definitions. Let $R=r^t$ be a prime power and p a prime, where $R|p$-1. Set $\underline{b}$ be an arrangement of all elements of the field F_R written as:

$$\underline{b}=(b_0b_1\ldots b_j\ldots b_{R-1}). \tag{1}$$

Definition. Let g be a generator of the multiplicative group $F_p^*=F_p\setminus\{0\}$ of the field F_p. The generalized Legendre sequence, or the R-th residual sequence of period p, denoted by $S_{\underline{b},g}(p,R)$, is a sequence $(s_0s_1\cdots s_i\cdots)\in F_R^{\infty}$, where

$$s_i=\begin{cases}0 & \text{if } i\equiv 0(\text{mod } p),\\ b_j & \text{if } i\equiv g^{j+Rk}(\text{mod } p),0\le j<R.\end{cases}$$

* Supported by the National Natural Science Foundation of China under Grant No.60173016 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035804 (国家重点基础研究发展规划 973 项目); Foundation of State Key Laboratory of Information Security (信息安全国家重点实验室对外开放基金)

WANG Ping was born in 1972. He is a Ph.D. candidate at the State Key Laboratory of Informational Security, the Chinese Academy of Sciences. His research interests are algebras and applied mathematics. **DAI Zong-duo** was born in 1941. She is a professor and doctoral supervisor of the State Key Laboratory of Informational Security, the Chinese Academy of Sciences. Her current research areas are algebras and cryptograph.

Fixing p and R, we simply denote $S_{\underline{b},g}(p,R)$ by $S_{\underline{b},g}$.

Let S_R be the set of arrangements of all elements of F_R. We discuss the transformations acting on S_R. Let μ be an integer such that (μ,R)=1. We define the μ-decimation of $\underline{b}$ as

$$\underline{b}^{(\mu)}=(b_0b_\mu\cdots b_{\mu j}\cdots b_{\mu(R-1)}),\quad \text{where if } j'\equiv j(\bmod R),\ \text{then } b_{j'}=b_j.$$

The transformation $L^\lambda(\underline{b})=(b_\lambda b_{\lambda+1}\cdots b_{p-1}b_0\cdots b_{\lambda-1})$ is called the left shift of $\underline{b}$. With the map $x\to x^r$ acting on each component of $\underline{b}$, we get another transformation $\delta(\underline{b})=(b_0{}^rb_1{}^r\cdots b_{R-1}{}^r)$. By multiplying each component of $\underline{b}$ with $\alpha\in F_R$, the transformation $\theta_\alpha(\underline{b})=(\alpha b_0\ \alpha b_1\cdots\alpha b_{R-1})$. Clearly, $\underline{b}^{(\mu)}$ ($(r,\mu)=1$), $L^\lambda(\underline{b}),\delta(\underline{b})$ and $\theta_\alpha(\underline{b})$ ($\alpha\neq0$) are still the arrangements over F_R. Similarly, we can define the corresponding generalized Legendre sequences $S_{\underline{b}^{(\mu)},g},S_{\delta(\underline{b}),g}$ and so on.

About these sequences above, we have some lemmas as follows.

Lemma 1[4]. Let λ and μ be two integers such that $(\lambda,p-1)=1$ and $\lambda\mu\equiv1(\bmod R)$. Then, $S_{\underline{b},g^\lambda}=S_{\underline{b}^{(\mu)},g}$.

So, we can fix g and simply denote $S_{\underline{b},g}$ by $S_{\underline{b}}$.

Lemma 2[4]. $S_{\underline{b}}{}^{(g^\lambda)}=S_{L^\lambda(\underline{b})},S_{\theta_\alpha(\underline{b})}=\alpha S_{\underline{b}}$ if $\alpha\neq0,S_{\delta(\underline{b})}=S_{\underline{b}}{}^r$.

About some invariable properties of linear complexity $L(S_{\underline{b}})$ of $S_{\underline{b}}$, by Lemma 2, we get the following results.

Corollary 1[4].

1. $L(S_{L^\lambda(\underline{b})})=L(S_{\theta_\alpha(\underline{b})})=L(S_{\delta(\underline{b})})=L(S_{\underline{b}})$.

2. For any given arrangement $\underline{b}$ over F_R, there always exists an arrangement $\underline{b}'=(01b_2'\cdots b_{R-1}')$ such that $L(S_{\underline{b}})=L(S_{\underline{b}'})$.

Then, we have the following:

Theorem 1. For any given arrangement $\underline{b}$, let $x=|\{\underline{b}'\in S_R\mid L(S_{\underline{b}'})=L(S_{\underline{b}})\}|$. Then, $tR(R\text{-}1)|x$.

Proof. Let G be the transformation group generated by the transformations L, θ_α and δ acting on S_R where α is a generator of F_R^*. For any given arrangement $\underline{b}$, denote the orbit of G acting on $\underline{b}$ by $\underline{b}^G$.

By Corollary 1, it is suffice to prove that $tR(R\text{-}1)\mid\underline{b}^G\mid$. It is clear that $L(\theta_\alpha(\underline{b}))=\theta_\alpha(L(\underline{b})),L(\delta(\underline{b}))=\delta(L(\underline{b}))$ and $\delta(\theta_\alpha(\underline{b}))=\theta_\alpha(\delta(\underline{b}))$. So, any element in G is of form $\delta^i\theta_\alpha{}^jL^k$, where $0\le i<t,0\le j<R-1,0\le k<R$. We discuss the stabilizer $G_{\underline{b}}$ of G fixing $\underline{b}$. For any given arrangement $\underline{b}$, there is an arrangement $\underline{c}$ of form $(01*\cdots*)$ in the orbit $\underline{b}^G$. Since $\underline{c}^G=\underline{b}^G$, we can assume that $\underline{b}=(01b_2\cdots b_{R-1})$. If $\delta^i(\theta_\alpha{}^j(L^k(\underline{b})))=\underline{b}$, only looking at the action of $\delta^i\theta_\alpha{}^jL^k$ on the first two components of $\underline{b}$, we easily know that j=k=0. Since the components of $\underline{b}$ contains all elements of F_R, i=0. Thus, $|\underline{b}^G|=|G|$. If $\delta^i\theta_\alpha{}^jL^k=\delta^{i'}\theta_\alpha{}^{j'}L^{k'}$, then $\delta^{i-i'}(\theta_\alpha{}^{j-j'}(L^{k-k'}(\underline{b})))=\underline{b}$. Hence, $i=i',j=j'$ and $k=k'$. So, $|\underline{b}^G|=|G|=tR(R-1)$. The result holds.

Let $F_p{}^{*R}=\{i^R\mid i\in F_p{}^*\}=<g^R>$. The number r can be regarded as an element of $F_p{}^*/F_p{}^{*R}$ under the canonical map. We denote the order of i in the group $F_p{}^*/F_p{}^{*R}$ by $\mathrm{Ord}_{F_p{}^*/F_p{}^{*R}}(i)$ (or simply $Ord(i)$). Then, the following conclusion is obvious.

Lemma 3[4]. Assume $t=r^r s,\ (r,s)=1$ and

$$r \equiv g^{r^c\mu+Rk} (\text{mod } p), 1 \le r^c\mu \le R, (r,\mu)=1, 0 \le c \le t. \tag{2}$$

Then $\text{Ord}(R)=r^d$, where $d=t-e$, $e=\min\{c+\tau, t\}$.

Lemma 4[2,4,8]. Let

$$K_{\underline{b}} = \{i \mid S_{\underline{b}}(\beta^i)=0, 0 \le i < p\} \subseteq F_p^*, \tag{3}$$

where β is an element of order p of the algebraic closure $\overline{F_r}$ of F_r. Then,

$$L(S_{\underline{b}}) = p-1-|K_{\underline{b}}|. \tag{4}$$

The values $f_j(\beta^i), 0 \le j < R, 0 \le i < p$, are considered in Refs.[4,7], where $f_j(x)$ is defined as the following polynomial

$$f_j(x) = \sum_{h \in <g^R>} x^{g^j h} (\text{mod } x^p-1), \tag{5}$$

where we view the power exponent $g^j h$ of x as the element in the multiplicative group F_p^*.

In the rest of this paper, we fix β as an element of order p in $\overline{F_r}$. Then, by (5), $f_j(\beta)$ is well defined.

Lemma 5[4,7]. Let $\underline{b}=(b_0 b_1 \cdots b_{R-1})$. Then,

1. $S_{\underline{b}}(x) = \sum_{0 \le j < R} b_j f_j(x) \ (\text{mod } x^p-1)$.
2. $f_j(\beta^{ih}) = f_j(\beta^i)$, for any $h \in <g^R>, i \in F_p^*$. Moreover, $\sum_{0 \le j < R} f_j(\beta) = -1$.
3. $S_{\underline{b}}(\beta^{ih}) = S_{\underline{b}}(\beta^i)$, for any $h \in <g^R>; S_b(\beta^{g^\lambda}) = \sum_{0 \le j < R} b_{j-\lambda} f_j(\beta), 0 \le \lambda < R; S_{\underline{b}}(1) = 0$.

For any $1 \le a \le t$, we define

$$M_{\underline{b},a} = \{g^\lambda \mid S_{\underline{b}}(\beta^{g^\lambda})=0, 0 \le \lambda < r^a\}. \tag{6}$$

Lemma 6. Let $Ord(R)=r^d$ and $e=t-d$. Then,

$$K_{\underline{b}} = \dot{\bigcup_{g^\lambda \in M_{\underline{b},e}}} g^\lambda <g^{r^e}>.$$

In particular,

$$|K_{\underline{b}}| = \frac{p-1}{r^e} |M_{\underline{b},e}|; |M_{\underline{b},e+i}| = r^i |M_{\underline{b},e}|, \forall\ 0 \le i \le d.$$

Then, $L(S_{\underline{b}}) = \frac{p-1}{r^e}(r^e - |M_{\underline{b},e}|)$.

Proof. First we prove that for any $i \in K_{\underline{b}}$, both ig^R and iR belong to $K_{\underline{b}}$. By Lemma 5, $S_{\underline{b}}(\beta^{ig^R}) = S_{\underline{b}}(\beta^i) = 0$. So, $ig^R \in K_{\underline{b}}$. Since

$$0 = S_{\underline{b}}(\beta^i)^R = \left(\sum_{0 \le j < R} b_j f_j(\beta^i)\right)^R = \sum_{0 \le j < R} b_j{}^R f_j(\beta^{iR}) = \sum_{0 \le j < R} b_j f_j(\beta^{iR}) = S_{\underline{b}}(\beta^{iR}),$$

$iR \in K_{\underline{b}}$. Hence, $K_{\underline{b}}$ must be the union of some cosets of $<R, g^R> = <g^{r^e}>$ in F_p^*. Since g is a generator of F_p^*, all these cosets are of the form $g^\lambda <g^{r^e}>$ where $g^\lambda \in M_{\underline{b},e}$. So, $K_{\underline{b}} = \dot{\bigcup_{g^\lambda \in M_{\underline{b},e}}} g^\lambda <g^{r^e}>$ and $|K_{\underline{b}}| = <g^{r^e}> \| M_{\underline{b},e}| = \frac{p-1}{r^e} |M_{\underline{b},e}|$.

Note that

$$K_{\underline{b}} = \dot{\bigcup_{g^\lambda \in M_{\underline{b},e}}} g^\lambda <g^{r^e}> = \dot{\bigcup_{0 \le j < \frac{p-1}{r^e}}} g^{jr^e} \cdot M_{\underline{b},e}.$$

Then,

$$M_{\underline{b},e+i} = M_{\underline{b},e+i} \cap K_{\underline{b}} = \dot{\bigcup}_{0 \le j < r^i - 1} g^{jr^e} \cdot M_{\underline{b},e}.$$

Hence, $|M_{\underline{b},e+i}| = r^i |M_{\underline{b},e}|$, for any $0 \le i \le d$. Then, $L(S_{\underline{b}}) = \frac{p-1}{r^e} |M_{\underline{b},e}|$.

Then, by Lemma 4 and Lemma 6, we have

Lemma 7. For any arrangement $\underline{b}$, $\frac{p-1}{r^e} \Big| L(S_{\underline{b}})$, where $e = t-d$, $Ord(R) = r^d$.

In Ref.[4], Dai *et al* gave the linear complexities of some special generalized Legendre sequences $S_{\underline{b}}$ where $\underline{b}$ are *a*-natural arrangements.

We give further conclusions about the distribution of linear complexities of other generalized Legendre sequences. Dais' result is mainly the following theorem:

Theorem A[4]. Let $R = r^t > 2$ be a prime power and p an odd prime such that $r \nmid t$ and $R \mid p-1$. Set $Ord_{F_p^* / F_p^{*R}}(r) = r^t$. Then

1. If $d=t$, then for any arrangement $\underline{b}$ over F_R, $L(S_{\underline{b}}) = p-1$.
2. If $1 \le d < t$, then for any $(t-d+1)$ – nature arrangement $\underline{b}$ over F_R, $L(S_{\underline{b}}) = p-1$.
3. If $d=0$, then for any t-nature arrangement $\underline{b}$, $L(S_{\underline{b}}) = p-1-\frac{p-1}{R}$.

Of course, for other arrangements $\underline{b}$, the corresponding sequences $S_{\underline{b}}$ may have the small linear complexities. However, with the help of computer, we discover that for most arrangements $\underline{b}$, the corresponding sequences $S_{\underline{b}}$ have the large linear complexities.

Let $U = \{\underline{u} = (u,\cdots,u) \mid u \in F_R\} \subseteq F_R^R$. Regard F_R^R as an addition group of vector space of dimension R over F_R. Then, U is regarded as a subgroup of F_R^R. For any $\underline{b} \in F_R^R$, $\underline{b}+U = \{\underline{b}+\underline{u} \mid u \in F_R\}$ is a coset of U in F_R^R.

We discuss the distribution of $L(S_{\underline{b}+\underline{u}})$ on $\underline{b}+U$ for any given arrangement $\underline{b}$.

Lemma 8. For any given $\underline{b} \in F_R^R$,

$$\sum_{\underline{u} \in U} |M_{\underline{b}+\underline{u},e}| \le r^e, \quad \text{where } e=t\text{-}d.$$

Proof.

$$\sum_{\underline{u} \in U} |M_{\underline{b}+\underline{u},e}| = \sum_{\underline{u} \in U} \left| \{\lambda \mid S_{\underline{b}+\underline{u}}(\beta^{g^\lambda}) = 0, 0 \le \lambda < r^e\} \right| = \left| \{(\lambda,\underline{u}) \mid S_{\underline{b}+\underline{u}}(\beta^{g^\lambda}) = 0, 0 \le \lambda < r^e, \underline{u} \in U\} \right|$$

$$= \sum_{0 \le \lambda < r^e} \left| \{\underline{u} \mid S_{\underline{b}}(\beta^{g^\lambda}) - u = 0, u \in F_R\} \right| \le \sum_{0 \le \lambda < r^e} 1 = r^e.$$

Lemma 9. For any given $\underline{b} \in F_R^R$, let $E_{\underline{b}}$ be the average value of $L(S_{\underline{b}+\underline{u}})$ on $\underline{b}+U$. Then,

$$E_{\underline{b}} \ge \frac{(p-1)(R-1)}{R}.$$

Proof. Let $Ord(R) = r^d, e = t-d$. Then,

$$E_{\underline{b}} = \frac{1}{|U|}\sum_{\underline{u}\in U} L(S_{\underline{b}+\underline{u}}) = \frac{1}{|U|}\sum_{\underline{u}\in U}\frac{p-1}{r^e}(r^e - |M_{\underline{b}+\underline{u},e}|)$$
$$\geq \frac{p-1}{Rr^e}(Rr^e - r^e) \qquad \text{(by Lemma 8)}$$
$$= \frac{(p-1)(R-1)}{R}.$$

Theorem 2. Assume $Ord(R) = r^d, 0 \leq d \leq t$. For any given arrangement $\underline{b}$, let $P_{\underline{b},l}$ be the probability of $L(S_{\underline{b}+\underline{u}}) = l$ for $\underline{u} \in U$.

(1) If *Ord(R)*=1, then $P_{\underline{b},p-1} + \frac{1}{2}P_{\underline{b},\frac{(p-1)(R-1)}{R}} \geq \frac{1}{2}$.

(2) If $Ord(R) = r^d, 0 < d < t$, then $P_{\underline{b},p-1} \geq 1 - \frac{1}{r^d}$,

(3) If $Ord(R) = r^t$, then $P_{\underline{b},p-1} = 1$.

Proof. Let *e=t-d*. For any given arrangement $\underline{b}$, denote $x_i = |\{\underline{u} \,||\, M_{\underline{b}+\underline{u},e}| = i, \underline{u} \in U\}|$. By Lemma 6, $x_i = \left|\{\underline{u} \,|\, L(S_{\underline{b}+\underline{u}}) = \frac{p-1}{r^e}(r^e - i), \underline{u} \in U\}\right|$. Thus,

$$P_{\underline{b},\frac{p-1}{r^e}(r^e-i)} = \frac{x_i}{R}. \tag{7}$$

By the definition of x_i and Lemma 7,

$$\sum_{0\leq i<r^e} x_i = R, \tag{8}$$

By Lemma 8,

$$\sum_{1\leq i<r^e} i \cdot x_i = \sum_{\underline{u}\in U} |M_{\underline{b}+\underline{u},e}| \leq r^e. \tag{9}$$

If *Ord(R)*=1, $r^e = R$. By (8) and (9),

$$R = r^t \geq \sum_{1\leq i<r^e} i \cdot x_i \geq x_1 + 2\sum_{1<i<r^e} x_i = x_1 + 2(R - x_0 - x_1).$$

So, $2x_0 + x_1 \geq R$. Then, $P_{\underline{b},p-1} + \frac{1}{2}P_{\underline{b},\frac{(p-1)(R-1)}{R}} = \frac{x_0}{R} + \frac{x_1}{2R} \geq \frac{1}{2}$. (1) holds.

If $Ord(R) = r^d, 0 < d < t$, by (8) and (9), $r^{t-d} \geq \sum_{1\leq i<r^e} i \cdot x_i \geq \sum_{1\leq i<r^e} x_i = R - x_0$. So, $x_0 \geq R - r^{t-d}$. Then, $P_{\underline{b},p-1} = \frac{x_0}{R} \geq 1 - \frac{1}{r^d}$. (2) holds.

By Theorem A, (3) holds.

Noting that the set of arrangements is the union of the above cosets like $\underline{b} + U$, we have

Corollary 2. For at least half of all of arrangements $\underline{b}$, $L(S_{\underline{b}})$ are at least $\frac{(p-1)(R-1)}{R}$. Further, if $Ord(R) = r^d$ with $d > 0$, then the probability of $L(S_{\underline{b}})$ equal to *p*-1 is at least $1 - \frac{1}{r^d}$.

Remark. Besides the natural arrangements, there are more other arrangements such that the corresponding sequences have large linear complexities. According to Theorem 2, one may find these sequences in the following way:

For any given arrangement $\underline{b}$, if the corresponding sequence has not large linear complexity, we can obtain new arrangement $\underline{b}'$ by adding $\underline{u}(\in U)$ onto the arrangement $\underline{b}$. After at most testing $\left[\frac{R}{2}\right]$ arrangements, we must find a new arrangement $\underline{b}'$ such that $S_{\underline{b}'}$ has the linear complexity not less than $\frac{(p-1)(R-1)}{R}$.

References:

[1] Damgaard, I. On the randomness of Legendre and Jacobi sequences. In: Advance in Cryptology(CRYPTO'88). Berlin, Germany: Spring-Verlag, 1990. 163~172.

[2] Ding, Cun-sheng, Helleseth, T., Shan, W. On the complexity of Legendre sequence. IEEE Transactions on IT, 1998,44(3): 1276~1278.

[3] Bromfield, A.J., Piper, F.C. Linear recursion properties of unrelated binary sequences. Discrete Applied Mathematics, 1990,27(2): 187~193.

[4] Dai, Zong-duo, Yang, Jun-hui, Gong, Guang, *et al*. On the linear complexity of generalized Legendre sequence. In: Helleseth, T., ed. Proceedings of the SETA2001. Spring-Verlag, 2001. 145~153.

[5] Ding, Cun-sheng. The differential cryptanalysis and design of the natural stream ciphers. In: Preneel, B., ed., Fast Software Encryption. LNCS 809, Berlin: Springer-Verlag, 1994. 101~115.

[6] Helleseth, T. Legendre sums and codes related to QR codes. Discrete applied Mathematics, 1992,35(1):107~113.

[7] Hu, Yu-pu, Wei, Shi-ming, Xiao, Guo-zhen. On the linear complexity of generalized Legendre/Jacobi sequences. Acta Electronica Sinica, 2000,28(2):113~117 (in Chinese).

[8] Lidl, R., Niederreiter, H. Finite Fields. In: Encyclopedia of Mathematics and Its Applications. Vol.20, Reading, MA: Addison-Wesley, 1983.

附中文参考文献：

[7] 胡予濮,魏仕民,肖国镇.广义 Legendre 序列和广义 Jacobi 序列的线性复杂度.电子学报,2000,28(2):113~117.

广义 **Legendre** 序列线性复杂度的分布

王 平, 戴宗铎

(中国科学院 研究生院 信息安全国家重点实验室,北京 100039)

摘要: 对广义 Legendre 序列线性复杂度的分布进行了估计,发现绝大多数广义 Legendre 序列有大的线性复杂度.给出了一个方法以得到具有大线性复杂度的广义 Legendre 序列.

关键词: 线性复杂度;广义 Legendre 序列

中图法分类号: TP309 文献标识码: A