J. Math. Crypt. **1** (2007), 283–296

DOI 10.1515 / JMC.2007.014

On the k-error linear complexity of cyclotomic sequences

Hassan Aly, Wilfried Meidl, and Arne Winterhof

Communicated by Ronald Cramer

Abstract. Exact values and bounds on the k-error linear complexity of p-periodic sequences which are constant on the cyclotomic classes are determined. This family of sequences includes sequences of discrete logarithms, Legendre sequences and Hall's sextic residue sequence.

Keywords. Pseudorandom sequences, k-error linear complexity, cyclotomic sequences, discrete logarithm, Legendre sequence, Hall's sextic residue sequences.

AMS classification. 94A55, 11T71.

1 Introduction

Let $p > 2$ be a prime and denote by $\mathbb{F}_p$ the finite field of order p which we identify with the set of integers $\{0, 1, \ldots, p-1\}$.

The *linear complexity* $L(\mathcal{S})$ of an N-periodic sequence $\mathcal{S} = \sigma_0, \sigma_1, \ldots$ over $\mathbb{F}_p$ is the smallest nonnegative integer L for which there exist coefficients $d_1, d_2, \ldots, d_L \in \mathbb{F}_p$ such that

$$\sigma_i + d_1\sigma_{i-1} + \cdots + d_L\sigma_{i-L} = 0 \quad \text{for all } i \geq L.$$

The linear complexity is of fundamental importance as a complexity measure for periodic sequences (see [14, 15, 16, 17, 8]). Motivated by security issues of stream ciphers, in [19] Stamp and Martin proposed a different measure of the complexity of periodic sequences, the *k-error linear complexity*, which is defined by

$$L_k(\mathcal{S}) = \min_{\mathcal{T}} L(\mathcal{T}),$$

where the minimum is taken over all N-periodic sequences $\mathcal{T} = \tau_0, \tau_1, \ldots$ over $\mathbb{F}_p$ for which the Hamming distance of the vectors $(\sigma_0, \sigma_1, \ldots, \sigma_{N-1})$ and $(\tau_0, \tau_1, \ldots, \tau_{N-1})$ is at most k. Evidently we have

$$N \geq L_0(\mathcal{S}) = L(\mathcal{S}) \geq L_1(\mathcal{S}) \geq L_2(\mathcal{S}) \geq \ldots \geq L_N(\mathcal{S}) = 0.$$

The concept of k-error linear complexity was built on the earlier concepts of *sphere complexity* $SC_k(\mathcal{S})$ introduced in the monograph [7] and *weight complexity* introduced in [4], see also [3, Chapter 2.3.4]. The sphere complexity $SC_k(\mathcal{S})$ of an N-periodic sequence over $\mathbb{F}_p$ can be defined by

$$SC_k(\mathcal{S}) = \min_{\mathcal{T}} L(\mathcal{T}),$$

Third author: A.W. was supported by the Austrian Science Fund (FWF) under the grants S8313 and P19004-N18.

where the minimum is taken over all N-periodic sequences $\mathcal{T} \neq \mathcal{S}$ over $\mathbb{F}_p$ for which the Hamming distance of the vectors $(\sigma_0, \sigma_1, \ldots, \sigma_{N-1})$ and $(\tau_0, \tau_1, \ldots, \tau_{N-1})$ is at most k. Obviously we have

$$L_k(\mathcal{S}) = \min(SC_k(\mathcal{S}), L(\mathcal{S})).$$

The weight complexity $WC_k(\mathcal{S})$ of $\mathcal{S}$ is the minimal linear complexity of all sequences with Hamming distance to $\mathcal{S}$ exactly k.

Let $d > 1$ be a divisor of $p-1$ and α a fixed primitive element of $\mathbb{F}_p$. Then the *cyclotomic classes of order* d give a partition of $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ defined by

$$D_0 = \{\alpha^{dn} \,:\, 0 \le n \le (p-1)/d - 1\} \quad \text{and} \quad D_j = \alpha^j D_0,\ 1 \le j \le d-1.$$

For fixed $c_0, c_1, \ldots, c_{d-1} \in \mathbb{F}_p$ the *cyclotomic sequence of order* d is the p-periodic sequence $\mathcal{C} = \zeta_0, \zeta_1, \ldots$ defined by

$$\zeta_i = \begin{cases} 0, & p|i, \\ c_j, & (i \bmod p) \in D_j,\ 0 \le j \le d-1, \end{cases} \qquad i = 0, 1, \ldots. \tag{1.1}$$

As p-periodic sequence, $\mathcal{C}$ is defined by its first p terms. Hence it is sufficient to define ζ_i for $0 \le i \le p-1$.
In the case that

$$c_j = j, \quad 0 \le j \le d-1,$$

we have

$$\zeta_i = \operatorname{ind}_d i, \quad 1 \le i \le p-1, \tag{1.2}$$

where $\operatorname{ind}_d i$ denotes the *discrete logarithm* modulo d of i, i.e. the unique j with $i = \alpha^{j_0}$ for some $j_0 \equiv j \bmod d$ and $0 \le j \le d-1$. Some cryptographic properties of the sequence $\mathcal{C}$ with (1.2) were analyzed in [5, 10, 12, 13, 21]. In particular, these results support the assumption of the hardness of the discrete logarithm problem. This paper provides further indications on how hard the discrete logarithm problem is. In the case $d = 2$ the sequence (1.2) is called *Legendre sequence*, see [6, 20]. The k-error linear complexity over $\mathbb{F}_p$ of the Legendre sequence $\mathcal{L}$ was determined for all k in [1],

$$L_k(\mathcal{L}) = \begin{cases} p, & k = 0, \\ (p+1)/2, & 1 \le k \le (p-3)/2, \\ 0, & k \ge (p-1)/2. \end{cases} \tag{1.3}$$

A *cyclotomic sequence of order* 4 defined with

$$c_0 = c_3 = 1 \text{ and } c_1 = c_2 = 0 \tag{1.4}$$

is investigated in [3, Chapter 8]. *Hall's sextic residue sequence* $\mathcal{H}$ [11, 9] is the cyclotomic sequence of order 6 with

$$c_0 = c_1 = c_3 = 1 \text{ and } c_2 = c_4 = c_5 = 0.$$

The main objectives of this paper are to find systematically sequences with high k-error linear complexity in view of their suitability for stream ciphers and to analyze some famous sequences suggested in the literature. In particular, we extend (1.3) to arbitrary cyclotomic sequences. Under a certain necessary restriction on the choice of the c_j we prove that

$$L_k(\mathcal{C}) = \frac{(d-1)(p-1)}{d} + 1, \quad 1 \le k \le \frac{p-1}{d} - 1.$$

For the above mentioned special examples we also prove explicit results on the k-error linear complexity for $k \ge (p-1)/d$.

2 Preliminary results

First we recall [2, Theorem 8].

Lemma 2.1. *Let $f(X) \in \mathbb{F}_p[X]$ be a polynomial of degree at most $p-1$ and $\mathcal{S} = \sigma_0, \sigma_1, \ldots$ the p-periodic sequence over $\mathbb{F}_p$ defined by*

$$\sigma_i = f(i) \quad \textit{for } 0 \le i \le p-1.$$

Then we have

$$L(\mathcal{S}) = \deg(f) + 1.$$

Next we prove a result on the stability of the linear complexity.

Lemma 2.2. *Let $\mathcal{S}$ be a p-periodic sequence over $\mathbb{F}_p$ and $0 \le k_0 \le (p-1)/2$. Then we have*

$$L_k(\mathcal{S}) = L_{k_0}(\mathcal{S}) \quad \textit{for } k_0 \le k \le p - L_{k_0}(\mathcal{S}) - k_0.$$

Proof. By the definition of the k-error linear complexity and by Lemma 2.1 for $0 \le m \le p-1$ there exists a polynomial $f_m(X) \in \mathbb{F}_p[X]$ of degree $L_m(\mathcal{S}) - 1$ and a subset $S_m \subseteq \mathbb{F}_p$ of cardinality at least $p-m$ such that $\sigma_i = f_m(i)$ for all $i \in S_m$. Hence, for any $k \ge k_0$ we have

$$f_k(i) - f_{k_0}(i) = 0 \quad \text{for all } i \in S_k \cap S_{k_0}$$

and

$$\deg(f_k - f_{k_0}) \le L_{k_0}(\mathcal{S}) - 1.$$

Since $|S_k \cap S_{k_0}| \ge p - k - k_0$ we have either $f_k(X) = f_{k_0}(X)$ or $p - k - k_0 \le \deg(f_k - f_{k_0}) \le L_{k_0}(\mathcal{S}) - 1$, or equivalently, either $L_k(\mathcal{S}) = L_{k_0}(\mathcal{S})$ or $k \ge p - L_{k_0}(\mathcal{S}) - k_0 + 1$. □

Now we describe the standard method for finding the unique polynomial $f(X) \in \mathbb{F}_p[X]$ of degree at most $p-1$ satisfying $f(i) = \zeta_i$ for all $i \in \mathbb{F}_p$.

Let α, d be as defined above, and put $\rho = \alpha^{(p-1)/d}$. First we construct the unique polynomial $g(X) = a_0 + a_1X + \cdots + a_{d-1}X^{d-1}$ of degree at most $d-1$ with $g(\rho^j) = c_j$. We consider the Vandermonde matrix

$$V = (\rho^{ij})_{i,j=0}^{d-1}.$$

The inverse of V is given by

$$V^{-1} = (d^{-1}\rho^{i(d-j)})_{i,j=0}^{d-1}.$$

Consequently the solution

$$(a_0, a_1, \ldots, a_{d-1}) = (c_0, c_1, \ldots, c_{d-1})V^{-1}$$

of the linear equation system $(X_0, X_1, \ldots, X_{d-1})V = (c_0, c_1, \ldots, c_{d-1})$ is explicitely given by

$$a_j = d^{-1}\sum_{i=0}^{d-1} c_i\rho^{i(d-j)},\ 0 \le j \le d-1.$$

Evidently the polynomial

$$\bar{f}(X) = g(X^{(p-1)/d}) = a_0 + a_1X^{\frac{p-1}{d}} + \cdots + a_{d-1}X^{(d-1)\frac{p-1}{d}} \tag{2.1}$$

satisfies $\bar{f}(i) = \zeta_i = c_j$ if $i^{(p-1)/d} = \rho^j$, i.e. $(i \bmod p) \in D_j$, for $i = 1, 2, \ldots, p-1$. Moreover, the polynomial

$$f(X) = a_0X^{p-1} + a_1X^{\frac{p-1}{d}} + \cdots + a_{d-1}X^{(d-1)\frac{p-1}{d}} \tag{2.2}$$

of degree at most $p-1$ satisfies $f(i) = \zeta_i$ for all $i = 0, 1, \ldots, p-1$.

3 General results on the k-error linear complexity

The following theorem indicates how to determine the exact value for the k-error linear complexity of a sequence defined by (1.1) for a certain range of k.

Theorem 3.1. *Let $p > 2$ be a prime, d a divisor of $p-1$, $c_0, c_1, \ldots, c_{d-1} \in \mathbb{F}_p$, α a primitive element of $\mathbb{F}_p$ and $\mathcal{C}$ the p-periodic sequence over $\mathbb{F}_p$ defined by (1.1). Put $\rho = \alpha^{(p-1)/d}$ and*

$$b_j = \sum_{i=0}^{d-1} c_i\rho^{ij}, \quad 0 \le j \le d-1.$$

Let t be the smallest index such that $b_t \neq 0$ then

$$L_k(\mathcal{C}) = p - t(p-1)/d \quad \textit{for} \quad 0 \le k \le t(p-1)/d.$$

Additionally, if $b_0 \neq 0$ and τ is the smallest index with $\tau \ge 1$ and $b_\tau \neq 0$, then

$$L(\mathcal{C}) = p \quad \textit{and} \quad L_k(\mathcal{C}) = p - \tau(p-1)/d \quad \textit{for} \quad 1 \le k \le \tau(p-1)/d - 1.$$

Proof. Note that $b_0 = da_0$ and $b_j = da_{d-j}$ for $1 \le j \le d-1$.

If t is the smallest index such that $b_t \neq 0$ then the corresponding polynomial (2.2) has degree $(d-t)(p-1)/d$. With Lemmas 2.1 and 2.2 we get the first assertion of the theorem.

If $b_0 \neq 0$ and τ is the smallest index with $\tau \ge 1$ and $b_\tau \neq 0$, then the polynomial (2.2) has degree $p-1$, and the polynomial (2.1) has degree $(d-\tau)(p-1)/d$. Consequently with Lemma 2.1 we have $L(\mathcal{C}) = p$, and since $\bar{f}(i) = \zeta_i$, $1 \le i \le p-1$, we have $L_1(\mathcal{C}) = p - \tau(p-1)/d$ since each polynomial that coincides with $\bar{f}(X)$ in at least $p-2$ positions is either equal to $\bar{f}(X)$ or has degree at least $p-2$. With Lemma 2.2 we obtain $L_k(\mathcal{C}) = L_1(\mathcal{C})$ for $1 \le k \le \tau(p-1)/d - 1$. □

Theorem 3.2. *For a p-periodic sequence $\mathcal{C}$ over $\mathbb{F}_p$ defined by (1.1) and an integer $0 \le t \le d$ we have*

$$L_k(\mathcal{C}) \le (d-t-1)(p-1)/d + 1 \quad \textit{for} \quad k \ge t(p-1)/d + 1.$$

Proof. We choose $d-t$ different cyclotomic cosets $D_{j_1}, \ldots, D_{j_{d-t}}$ and calculate the polynomial $h(X) = a_0 + a_1 X + \cdots + a_{d-t-1}X^{d-t-1}$ of degree at most $d-t-1$ which satisfies $h(\rho^{j_i}) = c_{j_i}$, $i = 1, \ldots, d-t$. Then the polynomial $g(X) = a_0 + a_1 X^{(p-1)/d} + \cdots + a_{d-t-1}X^{(d-t-1)(p-1)/d}$ satisfies $g(j) = \zeta_j$ for at least $(d-t)(p-1)/d = p - (t(p-1)/d + 1)$ different j with $0 \le j \le p-1$. With Lemma 2.1 we get the assertion. □

4 k-error linear complexity for some selected generators

4.1 Discrete logarithm sequences

Applying Theorems 3.1 and 3.2 and using ideas from [18, Chapter 8] we obtain the following results.

Theorem 4.1. *For $d > 1$ the sequence $\mathcal{C} = \zeta_0, \zeta_1, \ldots$ defined by (1.2) with $\zeta_0 = 0$ satisfies*

$$L_k(\mathcal{C}) = \begin{cases} p & : \quad k = 0 \\ (d-1)(p-1)/d + 1 & : \quad 1 \le k \le (p-1)/d - 1 \\ 0 & : \quad k \ge (d-1)(p-1)/d. \end{cases}$$

For $d > 3$ and $(p-1)/d < k \le (d-1)(p-1)/(2d)$ we have

$$\frac{(d-1)(p-1)}{d} - 2k + 1 \le L_k(\mathcal{C}) \le \frac{(d-1-\lfloor d(k-1)/(p-1) \rfloor)(p-1)}{d} + 1.$$

Proof. With

$$b_0 = \sum_{j=0}^{d-1} c_j = \sum_{j=0}^{d-1} j = d(d-1)/2 \neq 0$$

and

$$\begin{aligned}(\rho-1)^2 b_1 &= (\rho-1)^2 \sum_{j=0}^{d-1} c_j \rho^j = (\rho-1)^2 \sum_{j=0}^{d-1} j\rho^j \\ &= \rho - d\rho^d + (d-1)\rho^{d+1} = d(\rho-1) \neq 0,\end{aligned}$$

Theorem 3.1, and the fact that the cyclotomic sequence produces $(d-1)(p-1)/d$ nonzero terms per period we obtain the first part of the theorem. The upper bound of the second part follows from Theorem 3.2.

Finally, we prove the lower bound of the second part. Let $f(X) \in \mathbb{F}_p[X]$ be a polynomial with $f(i) = \zeta_i = \mathrm{ind}_d\, i$ for at least $(d-1)(p-1)/d - k$ elements $1 \le i \le p-1$ with $i \notin C_{d-1}$. For at least $(d-1)(p-1)/d - 2k$ of these elements we also have

$$f(\alpha i) = \mathrm{ind}_d\, (\alpha i) = 1 + \mathrm{ind}_d\, i = 1 + f(i).$$

Hence, the polynomial $F(X) = f(\alpha X) - f(X) - 1$ of degree at most $\deg(f)$ has at least $(d-1)(p-1)/d - 2k$ zeros. Since $F(0) = -1 \neq 0$ we get $\deg(f) \ge \deg(F) \ge (d-1)(p-1)/d - 2k$ and the result follows by Lemma 2.1. □

Theorem 4.1 gives only a nontrivial lower bound if $k < (d-1)(p-1)/2d$. Next we prove a lower bound which is nontrivial for all $k < (d-1)(p-1)/d$.

Theorem 4.2. *We have*

$$L_k(\mathcal{C}) \ge \frac{(p-1-k)((d-1)(p-1)-dk)}{2(d-1)(p-1)} + 1.$$

Proof. Let $S \subseteq \mathbb{F}_p^*$ be any set of cardinality $|S| \ge p-1-k$ and $f(X) \in \mathbb{F}_p[X]$ any polynomial with

$$f(i) = \zeta_i, \quad i \in S.$$

Let us consider the set

$$D = \{a = i^{-1}j : \mathrm{ind}_d\, a \neq 0,\ i, j \in S\}.$$

We have $|D| \le (d-1)(p-1)/d$ and there exists an $a \in D$ such that there are at least

$$\frac{|S|(|S| - (p-1)/d)}{|D|} \ge \frac{d(p-1-k)(p-1-k-(p-1)/d)}{(d-1)p}$$

representations $a = i^{-1}j$, $i, j \in S$. Select this a and let

$$R = \{i \in \mathbb{F}_p^* : f(i) = \zeta_i \text{ and } f(ai) = \zeta_{ai}\}.$$

We see that $|R| \ge (p-1-k)((d-1)(p-1)-dk)/(d-1)p$.

Moreover, we have either $\mathrm{ind}_d\, (ai) = \mathrm{ind}_d\, a + \mathrm{ind}_d\, i$ or $\mathrm{ind}_d\, (ai) = -d + \mathrm{ind}_d\, a + \mathrm{ind}_d\, i$. Hence, at least one of the polynomials

$$h_1(X) = f(aX) - f(X) - \mathrm{ind}_d\, a \text{ and } h_2(X) = f(aX) - f(X) + d - \mathrm{ind}_d\, a$$

has at least $|R|/2$ zeros. Since $h_1(0) = p - \text{ind}_d\, a \neq 0$ and $h_2(0) = d - \text{ind}_d\, a \neq 0$ we get

$$\deg f \geq \max\{\deg h_1, \deg h_2\} \geq |R|/2$$

and the result follows by Lemma 2.1. □

For concrete values of d we can improve the lower bounds of Theorems 4.1 and 4.2. We present the result for $d = 3$.

Theorem 4.3. *For $p > 7$ and $d = 3$ the sequence $\mathcal{C}$ of Theorem 4.1 satisfies*

$$L_k(\mathcal{C}) = \begin{cases} p & : \quad k = 0 \\ 2(p-1)/3 + 1 & : \quad 1 \leq k \leq (p-1)/3 - 1 \\ (p-1)/3 + 1 & : \quad (p-1)/3 + 1 \leq k < (p-1)/2 \\ 0 & : \quad k \geq 2(p-1)/3, \end{cases}$$

and additionally

$$4(p-1)/9 + 1 \leq L_{(p-1)/3}(\mathcal{C}) \leq 2(p-1)/3 + 1.$$

Proof. For $k \leq (p-1)/3 - 1$ and $k \geq 2(p-1)/3$ the result immediately follows from Theorem 4.1.

Next we assume $k \geq (p-1)/3 + 1$ and annotate that the polynomials

$$\begin{aligned} g_0(X) &= \frac{1}{\rho - 1}\left(\rho - 2 + \frac{1}{\rho}X^{(p-1)/3}\right), \\ g_1(X) &= \frac{2}{\rho^2 - 1}\left(-1 + X^{(p-1)/3}\right), \\ g_2(X) &= \frac{1}{\rho - 1}\left(-1 + X^{(p-1)/3}\right), \end{aligned}$$

satisfy

$$\zeta_j = g_i(j) \quad \text{for } j \in \mathbb{F}_p^* \setminus D_i,$$

but

$$\zeta_j \neq g_i(j) \quad \text{for } j \in D_i \cup \{0\},$$

$i = 0, 1, 2$. (Note that if $p = 7$ we may have $\rho = 2$ and thus $g_0(0) = 0$.) From Lemma 2.1 we get $L_k(\mathcal{C}) \leq \deg g_i + 1 = (p-1)/3 + 1$. We remark that the polynomials $g_i(X)$ can easily be obtained with the method described in Section 2 for finding the unique polynomial $\bar{f}(X) \in \mathbb{F}_p[X]$ of smallest degree satisfying $f(j) = \zeta_j$ for all $j \in \mathbb{F}_p^*$.

In order to prove the theorem it remains to show that $L_{(p-1)/3}(\mathcal{C}) \geq 4(p-1)/9 + 1$, and that $L_k(\mathcal{C}) \geq (p-1)/3 + 1$ for $k < (p-1)/2$.

Let $\mathcal{T} = \tau_0, \tau_1, \ldots,$ be any p-periodic sequence obtained from $\mathcal{C}$ by at most k changes per period. Let $t(X) \in \mathbb{F}_p[X]$ be the polynomial with $t(j) = \tau_j$, $0 \leq j \leq p-1$. We obtain that $t(j) = g_i(j)$ for at least $2(p-1-k)/3$ elements j of $\mathbb{F}_p$ for an appropriate

choice of i, i.e., the polynomial $h(X) = t(X) - g_i(X)$ has at least $2(p-1-k)/3$ zeros. If we put $k = (p-1)/3$, then by the above considerations we have $t(X) \neq g_i(X)$ and thus $h(X)$ is not the zero polynomial. Consequently we must have $\deg(h) = \deg(t) \geq 2(p-1-k)/3 = 4(p-1)/9$ and thus $L_{(p-1)/3}(\mathcal{C}) \geq 4(p-1)/9+1$. Trivially we have the upper bound $L_{(p-1)/3}(\mathcal{C}) \leq L_{(p-1)/3-1}(\mathcal{C}) = 2(p-1)/3+1$.
For $k < (p-1)/2$ we have either $h(X) \equiv 0$ and thus $\deg(t) = \deg(g_i) = (p-1)/3$ or $\deg(h) = \deg(t) \geq 2(p-1-k)/3 > (p-1)/3$ and we have $L_k(\mathcal{C}) \geq (p-1)/3+1$. □

4.2 Cyclotomic sequences of order 4

Theorem 4.4. *The cyclotomic sequences $\mathcal{C}$ of order 4 defined by (1.1), and (1.2) for $p \neq 5, 17$ or (1.4), respectively, satisfy*

$$L_k(\mathcal{C}) = \begin{cases} p & : \quad k = 0 \\ 3(p-1)/4+1 & : \quad 1 \leq k \leq (p-1)/4-1 \\ (p-1)/2+1 & : \quad (p-1)/4+1 \leq k < (p-1)/3 \\ 0 & : \quad k \geq (p-1)/2. \end{cases}$$

Additionally we have

$$9(p-1)/16+1 \leq L_{(p-1)/4}(\mathcal{C}) \leq 3(p-1)/4+1,$$

and

$$(p-1)/4+1 \leq L_k(\mathcal{C}) \leq (p-1)/2+1 \text{ for } (p-1)/3 \leq k < (p-1)/2.$$

Proof. Since

$$\sum_{j=0}^{d-1} c_j = 2 \neq 0 \quad \text{and} \quad \sum_{j=0}^{d-1} c_j \rho^j = 1-\rho$$

for the sequence (1.2) with $d = 4$, and

$$\sum_{j=0}^{d-1} c_j = 6 \neq 0 \quad \text{and} \quad \sum_{j=0}^{d-1} c_j \rho^j = -2(\rho+1)$$

for the sequence (1.4), the cyclotomic sequence of order 4 satisfies $L(\mathcal{C}) = p$ and $L_k(\mathcal{C}) = 3(p-1)/4+1$ for $1 \leq k \leq (p-1)/4-1$ by Theorem 3.1.
For $0 \leq i \leq 3$ let $g_i(X) \in \mathbb{F}_p[X]$ be the unique polynomial of degree at most $(p-1)/2$ satisfying

$$g_i(j) = \zeta_j, \quad j \in \mathbb{F}_p^* \setminus D_i,$$

where ζ_j is defined with (1.2) for $d = 4$ and (1.4), respectively. For the sequence (1.2)

we have

$$\begin{aligned} g_0(X) &= \frac{1}{2\rho}\left(4\rho - 1 - 2X^{(p-1)/4} - X^{(p-1)/2}\right), \\ g_1(X) &= \frac{1}{2}\left(4 - \rho - 2X^{(p-1)/4} + (\rho-2)X^{(p-1)/2}\right), \\ g_2(X) &= \frac{1}{2\rho}\left(2\rho + 1 - 2X^{(p-1)/4} - (2\rho-1)X^{(p-1)/2}\right), \\ g_3(X) &= \frac{1}{2}\left(\rho + 2 - 2X^{(p-1)/4} - \rho X^{(p-1)/2}\right), \end{aligned}$$

and for the sequence (1.4),

$$\begin{aligned} g_0(X) &= \frac{1}{4}\left(\rho + 1 + 2\rho X^{(p-1)/4} + (\rho-1)X^{(p-1)/2}\right), \\ g_1(X) &= \frac{1}{4}\left(\rho + 3 + 2X^{(p-1)/4} - (\rho+1)X^{(p-1)/2}\right), \\ g_2(X) &= \frac{1}{4}\left(3 - \rho + 2\rho X^{(p-1)/4} + (1-\rho)X^{(p-1)/2}\right), \\ g_3(X) &= \frac{1}{4}\left(1 - \rho + 2X^{(p-1)/4} + (\rho+1)X^{(p-1)/2}\right). \end{aligned}$$

It is easy to check that $g_i(X)$ satisfies $g_i(0) \neq 0$ and $\deg(g_i) = (p-1)/2$ (since $p \neq 5, 17$ for the first sequence). Consequently we can apply the same technique as in the proof of Theorem 4.3 to prove the result for $(p-1)/4 + 1 \leq k < (p-1)/3$ and $k = (p-1)/4$.

Moreover the existence of the (unique) polynomials $b_0(X), b_1(X)$ of degree $(p-1)/4$ that satisfy

$$b_0(j) = \zeta_j \text{ if } j \in D_0 \cup D_2$$

and

$$b_1(j) = \zeta_j \text{ if } j \in D_1 \cup D_3,$$

enables us to use this technique for a further step. We have

$$\begin{aligned} b_0(X) &= 1 - X^{(p-1)/4}, \\ b_1(X) &= 2 - \rho^{-1}X^{(p-1)/4}, \end{aligned}$$

or

$$\begin{aligned} b_0(X) &= \frac{1}{2}\left(1 + X^{(p-1)/4}\right) \\ b_1(X) &= \frac{1}{2}\left(1 + \rho X^{(p-1)/4}\right), \end{aligned}$$

respectively. Suppose that $\mathcal{T} = \tau_0, \tau_1, \ldots$ is a p-periodic sequence obtained from $\mathcal{C}$ by at most k changes per period and let $t(X)$ be the polynomial with $t(j) = \tau_j$, $0 \leq j \leq$

$p-1$. Then for at least one $i \in \{0,1\}$ we have $t(j) = b_i(j)$ for at least $(p-1-k)/2$ elements $j \in \mathbb{F}_p$. Then the polynomial $h(X) = b_i(X) - t(X)$ has at least $(p-1-k)/2$ zeros. Hence, $h(X) \equiv 0$ and thus $\deg(t) = \deg(b_i) = (p-1)/4$ or $\deg(h) = \deg(t) \geq (p-1-k)/2 > (p-1)/4$. As a consequence we have $L_k(\mathcal{C}) \geq (p-1)/4 + 1$ if $k < (p-1)/2$. □

4.3 Hall's sextic residue sequence

For Hall's sextic residue sequence we can show the following result.

Theorem 4.5. *For the k-error linear complexity over $\mathbb{F}_p$, $p > 7$, of Hall's sextic residue sequence $\mathcal{H}$ we have*

$$\begin{array}{lcl}
L_k(\mathcal{H}) = p & : & k = 0, \\
L_k(\mathcal{H}) = 5(p-1)/6 + 1 & : & 1 \leq k \leq (p-1)/6 - 1, \\
25(p-1)/36 < L_k(\mathcal{H}) \leq 5(p-1)/6 + 1 & : & k = (p-1)/6, \\
L_k(\mathcal{H}) = 2(p-1)/3 + 1 & : & (p-1)/6 < k < (p-1)/5, \\
2(p-1)/3 - 2k/3 < L_k(\mathcal{H}) \leq 2(p-1)/3 + 1 & : & (p-1)/5 \leq k < (p-1)/4, \\
(p-1)/3 < L_k(\mathcal{H}) \leq 2(p-1)/3 + 1 & : & (p-1)/4 \leq k < (p-1)/3, \\
(p-1)/6 < L_k(\mathcal{H}) \leq (p+1)/2 & : & k = (p-1)/3, \\
(p-1)/6 < L_k(\mathcal{H}) \leq (p-1)/3 + 1 & : & (p-1)/3 < k < (p-1)/2, \\
L_k(\mathcal{H}) = 0 & : & k \geq (p-1)/2.
\end{array}$$

Proof. Since

$$\sum_{j=0}^{d-1} c_j = 3 \neq 0 \quad \text{and} \quad \sum_{j=0}^{d-1} c_j \rho^j = 1 + \rho + \rho^3 = \rho \neq 0,$$

we obtain $L(\mathcal{H}) = p$ and $L_k(\mathcal{H}) = 5(p-1)/6 + 1$ for $1 \leq k \leq (p-1)/6 - 1$ by Theorem 3.1. Theorem 3.2 yields $L_k(\mathcal{H}) \leq 2(p-1)/3 + 1$ for $k \geq (p-1)/6 + 1$ and thus also for $k \geq (p-1)/4$. Since $\mathcal{H}$ has exactly $(p-1)/2$ nonzero terms per period we have $L_k(\mathcal{H}) = 0$ if and only if $k \geq (p-1)/2$.

The polynomial

$$g_{1,2}(X) = \frac{\rho^2}{\rho+1} X^{(p-1)/6} + X^{(p-1)/3} - \frac{\rho^2}{\rho+1} X^{(p-1)/2}$$

satisfies

$$g_{1,2}(j) = \zeta_j, \quad j \in \mathbb{F}_p \setminus (D_1 \cup D_2),$$

and the polynomial

$$g_{1,4}(X) = \frac{1}{\rho+1} \left(\rho + X^{(p-1)/3} \right)$$

satisfies

$$g_{1,4}(j) = \zeta_j, \quad j \in \mathbb{F}_p^* \setminus (D_1 \cup D_4).$$

Consequently $L_k(\mathcal{H}) \le (p-1)/2+1$ if $k \ge (p-1)/3$ and $L_k(\mathcal{H}) \le (p-1)/3+1$ if $k \ge (p-1)/3+1$.
From the table given below we see that the polynomials $g_i(X)$, $i = 0, \ldots, 5$, of degree at most $2(p-1)/3$ with

$$g_i(j) = \zeta_j, \quad j \in \mathbb{F}_p^* \setminus D_i,$$

satisfy $g_i(0) \neq 0$ and $\deg(g_i) = 2(p-1)/3$. (Here we need $p > 7$.) Consequently we again can apply the technique of the proof of Theorem 4.3 and obtain $L_{(p-1)/6}(\mathcal{H}) \ge 25(p-1)/36+1$, and $L_k(\mathcal{H}) \ge 2(p-1)/3+1$ for $k < (p-1)/5$ which yields $L_k(\mathcal{H}) = 2(p-1)/3+1$ for $(p-1)/6+1 \le k < (p-1)/5$.
The following remains to be shown: (I) $L_k(\mathcal{H}) \ge 2(p-1)/3+1-2k/3$ for $(p-1)/5 \le k < (p-1)/4$, (II) $L_k(\mathcal{H}) \ge (p-1)/3+1$ for $k < (p-1)/3$, and (III) $L_k(\mathcal{H}) \ge (p-1)/6+1$ for $k < (p-1)/2$. We will prove (I), (II) and (III) by extending the technique of the proof of Theorem 4.3.
(I) We consider the 6 different polynomials

$$g_{i_1,i_2}(X) \in \mathbb{F}_p[X], (i_1,i_2) \in \{(0,1),(1,2),(2,3),(3,4),(4,5),(0,5)\},$$

of degree at most $(p-1)/2$, which satisfy

$$g_{i_1,i_2}(j) = \zeta_j, \quad j \in \mathbb{F}_p^* \setminus (D_{i_1} \cup D_{i_2}),$$

and observe that all of these polynomials are of degree $(p-1)/2$. W.l.o.g. suppose that $g_{i_1,i_2}(X)$ also satisfies $g_i(\bar{j}) = \zeta_{\bar{j}}$ for an element $\bar{j} \in D_{i_1}$. Then among the considered polynomials we can choose a polynomial g such that $g(j) = \zeta_j$ for $j \neq 0$ and for all $j \notin D_{i_2} \cup D_{i_3}$, $i_3 \neq i_1, i_2$. Then the polynomial $h(X) = g_{i_1,i_2}(X) - g(X)$ has at least $(p-1)/2+1$ solutions which is not possible. Consequently $g_{i_1,i_2}(j) \neq \zeta_j$ if $j \in D_{i_1} \cup D_{i_2}$, i.e. we have $g_i(j) \neq \zeta_j$ for at least $(p-1)/3$ elements of $\mathbb{F}_p$.

Let $\mathcal{T} = \tau_0, \tau_1, \ldots$ be a sequence obtained from $\mathcal{H}$ by at most $k < (p-1)/4$ changes, and let $t(X)$ be the polynomial with $t(j) = \tau_j$. Then $t(X) \neq g_{i_1,i_2}(X)$ for all considered pairs (i_1,i_2), and for at least one pair (i_1,i_2) we have $t(j) = g_{i_1,i_2}(j)$ for at least $2(p-1-k)/3$ elements j of $\mathbb{F}_p$. Consequently $h(X) = t(X) - g_{i_1,i_2}(X)$ has at least $2(p-1-k)/3$ zeros, and hence $\deg(h) \ge 2(p-1-k)/3$. Note that since $2(p-1-k)/3 > (p-1)/2$ as long as $k < (p-1)/4$ we have $\deg(h) = \deg(t) \ge 2(p-1-k)/3$ which completes the proof of (I).
(II) Let $b_0(X)$ and $b_1(X)$ be the (unique) polynomials of degree $(p-1)/3$ for which we have $b_0(j) = \zeta_j$ if $j \in D_0 \cup D_2 \cup D_4$ and $b_1(j) = \zeta_j$ if $j \in D_1 \cup D_3 \cup D_5$, and let again $t(X)$ be a polynomial with $t(j) = \zeta_j$ for at least $p-k$ terms. Then for at least one $i \in \{0,1\}$ we have $b_i(j) = t(j)$ for at least $(p-1-k)/2$ elements of $\mathbb{F}_q$. Suppose that the degree of $t(X)$ is smaller than $(p-1)/3$. Then the polynomial $h(X) = b_i(X) - t(X)$ of degree $(p-1)/3$ has at least $(p-1-k)/2$ zeros which is a contradiction as long as $k < (p-1)/3$. This completes the proof of (II).
(III) Let $d_0(X), d_1(X), d_2(X)$ be the (unique) polynomials of degree exactly $(p-1)/6$ and $d_0(j) = \zeta_j$ if $j \in D_0 \cup D_2$, $d_1(j) = \zeta_j$ if $j \in D_1 \cup D_4$ and $d_2(j) = \zeta_j$ if $j \in D_3 \cup D_5$. For at least one $i \in \{0,1,2\}$, a polynomial $t(X)$ with $t(j) = \zeta_j$ for at least $p-k$ terms satisfies $t(j) = d_i(j)$ for at least $(p-1-k)/3$ elements of $\mathbb{F}_q$. Suppose that the degree of $t(X)$ is smaller than $(p-1)/6$. Then the polynomial $h(X) = d_i(X) - t(X)$ of degree $(p-1)/6$ has at least $(p-1-k)/3$ zeros which is a contradiction as long as $k < (p-1)/2$. □

Appendix to the proof of Theorem 4.5:

$$
\begin{aligned}
g_0(X) &= \frac{1}{6}\Big((3-\rho)-(1+2\rho^2)X^{(p-1)/6}-2\rho^2X^{(p-1)/3}\\
&\quad -(1+\rho)X^{(p-1)/2}+X^{2(p-1)/3}\Big),\\
g_1(X) &= \frac{1}{3}\Big(1+X^{(p-1)/3}+X^{2(p-1)/3}\Big),\\
g_2(X) &= \frac{1}{6\rho}\Big((3\rho-1)+(1+\rho)X^{(p-1)/6}+2X^{(p-1)/3}\\
&\quad -(1+\rho)X^{(p-1)/2}+\rho(\rho+2)X^{2(p-1)/3}\Big),\\
g_3(X) &= \frac{1}{6}\Big((3+\rho)-(1+2\rho^2)X^{(p-1)/6}+2X^{(p-1)/3}-(1+\rho)X^{(p-1)/2}\\
&\quad +(1+2\rho)X^{2(p-1)/3}\Big),\\
g_4(X) &= \frac{1}{3}\Big(2-\rho^2X^{(p-1)/3}+\rho X^{2(p-1)/3}\Big),\\
g_5(X) &= \frac{1}{6\rho}\Big((3\rho+1)+(1+\rho)X^{(p-1)/6}+2\rho X^{(p-1)/3}\\
&\quad -(1+\rho)X^{(p-1)/2}+\rho^2X^{2(p-1)/3}\Big),\\
g_{0,1}(X) &= \frac{1}{\rho+1}\left(1+\frac{1}{\rho}X^{(p-1)/6}+\frac{1}{\rho}X^{(p-1)/3}-\rho X^{(p-1)/2}\right),\\
g_{2,3}(X) &= \frac{1}{\rho+1}\left(\frac{(\rho-1)(\rho+2)}{2\rho}+(2-\rho)X^{(p-1)/6}-X^{(p-1)/3}+\right.\\
&\quad \left.\frac{(\rho-1)(1-2\rho)}{2}X^{(p-1)/2}\right),\\
g_{3,4}(X) &= \frac{1}{3}\Big(3+(\rho-2)X^{(p-1)/6}+(3-3\rho)X^{(p-1)/3}\\
&\quad +(2\rho-1)X^{(p-1)/2}\Big),\\
g_{4,5}(X) &= \frac{1}{\rho+1}\left(\frac{\rho^2}{\rho-1}+X^{(p-1)/6}-\frac{1}{\rho-1}X^{(p-1)/3}-X^{(p-1)/2}\right),\\
g_{0,5}(X) &= \frac{1}{2}\Big(1-X^{(p-1)/2}\Big).
\end{aligned}
$$

Acknowledgments. The authors wish to thank Tanja Lange for her very helpful comments and suggestions.

References

[1] H. Aly and A. Winterhof, *On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov sequences*, Designs, Codes and Cryptography 40 (2006), pp. 369–374.

[2] S. Blackburn, T. Etzion, and K. Paterson, *Permutation polynomials, de Bruijn sequences, and linear complexity*, Journal of Combinatorial Theory, Series A 76 (1996), pp. 55–82.

[3] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. North-Holland Publishing Co., Amsterdam, 1998.

[4] C. Ding, *Lower bounds on the weight complexity of cascaded binary sequences*. Advances in Cryptology, Lecture Notes in Computer Science 453, pp. 39–43. Springer-Verlag, Berlin, 1991.

[5] C. Ding and T. Helleseth, *On cyclotomic generator of order r*, Information Processing Letters 66 (1998), pp. 21–25.

[6] C. Ding, T. Helleseth, and W. Shan, *On the linear complexity of Legendre sequences*, IEEE Transactions on Information Theory 44 (1998), pp. 1276–1278.

[7] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science 561. Springer-Verlag, Berlin, 1991.

[8] A. Topuzoğlu and A. Winterhof, *Topics in Geometry, Coding Theory and Cryptography (A. Garcia and H. Stichtenoth, Eds.)*, Algebra and Applications 6, ch. Pseudorandom sequences, pp. 135–166, Springer-Verlag,, Dordrecht, 2007.

[9] J-H. Kim and H-Y Song, *On the linear complexity of Hall's sextic residue sequences*, IEEE Transactions on Information Theory 47 (2001), pp. 2094–2096.

[10] S. Konyagin, T. Lange, and I. Shparlinski, *Linear complexity of the discrete logarithm*, Designs, Codes and Cryptography 28 (2003), pp. 135–146.

[11] Jr. M. Hall, *A survey of difference sets*. Proceedings of the American Mathematical Society, 7, pp. 975–986, 1956.

[12] W. Meidl and A. Winterhof, *Lower bounds on the linear complexity of the discrete logarithm in finite fields*, IEEE Transactions on Information Theory 47 (2001), pp. 2807–2811.

[13] ———, *On the autocorrelation of cyclotomic generators*. Proceedings of The Seventh International Conference on Finite Fields and Applications - F_q7(Toulouse 2003) (G.L. Mullen, A. Poli, and H. Stichtenoth, eds.), Lecture Notes in Computer Science 2948, pp. 1–11. Springer-Verlag, Berlin, 2004.

[14] H. Niederreiter, *Some computable complexity measures for binary sequences*. Proceedings of The International Conference on Sequences and Their Applications - SETA98 (C. Ding, T. Helleseth, and H. Niederreiter, eds.), pp. 67–78. Springer-Verlag, London, 1999.

[15] ———, *Linear complexity and related complexity measures for sequences*. Progress in Cryptology – Indocrypt 2003 (T. Johansson and S. Maitra, eds.), Lecture Notes in Computer Science 2904, pp. 1–17. Springer-Verlag, Berlin, 2003.

[16] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Springer-Verlag, Berlin, 1986.

[17] ———, *Contemporary Cryptology: The Science of Information Integrity (G.J. Simmons, Ed.)*, ch. Stream ciphers, pp. 65–134, IEEE Press, New York, 1992.

[18] I. Shparlinski, *Cryptographic applications of analytic number theory. Complexity lower bounds and pseudorandomness*, Progress in Computer Science and Applied Logic 22. Birkhäuser Verlag, Basel, 2003.

[19] M. Stamp and C. F. Martin, *An algorithm for the k-error linear complexity of binary sequences with period 2^n*, IEEE Transactions on Information Theory 39 (1993).

[20] R. J. Turyn, *The linear generation of Legendre sequence*, Journal of the Society of Industrial Applied Mathematics 12 (1964).

[21] A. Winterhof, *Coding, cryptography and combinatorics*, Progress in Computer Science and Applied Logic 23, ch. A note on the linear complexity profile of the discrete logarithm in finite fields, pp. 359–367, Birkhäuser Verlag, Basel, 2004.

Received 1 June, 2006; revised 15 November, 2006

Author information

Hassan Aly, Department of Mathematics, Faculty of Science, Cairo University, Giza, Egypt.
Email: haly@kfu.edu.sa

Wilfried Meidl, Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey.
Email: wmeidl@sabanciuniv.edu

Arne Winterhof, Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, A-4040 Linz, Austria.
Email: arne.winterhof@oeaw.sc.at