On the Linear Complexity of Legendre-Sidelnikov Sequences

Ming Su

Nankai University, China

Emerging Applications of Finite Fields, Linz, Dec. 12

Outline

Background

- Legendre Sequence

  For a prime $p > 2$ let (s_n) be the *Legendre sequence* defined as

$$s_n = \begin{cases} 1, & \left(\frac{n}{p}\right) = -1, \\ 0, & \textit{otherwise}, \end{cases} \qquad n \geq 0,$$

  where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

- Sidelnikov Sequence

  Let q be an odd prime power, g a primitive element of $\mathbb{F}_q$, and let η denote the *quadratic character* of $\mathbb{F}_q$, i.e., $\eta(g^i) = (-1)^i, \quad i = 0, 1, \ldots, q-2$. Then the *Sidel'nikov*(Lempel-Cohn-Eastman) *sequence* is defined:

$$s_n = \begin{cases} 1, & \text{if } \eta(g^n + 1) = -1, \\ 0, & \text{otherwise}, \end{cases} \qquad n = 0, 1, \ldots.$$

Background

- Legendre Sequence

  For a prime $p > 2$ let (s_n) be the *Legendre sequence* defined as

$$s_n = \begin{cases} 1, & \left(\frac{n}{p}\right) = -1, \\ 0, & \textit{otherwise}, \end{cases} \qquad n \geq 0,$$

  where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

- Sidelnikov Sequence

  Let q be an odd prime power, g a primitive element of $\mathbb{F}_q$, and let η denote the *quadratic character* of $\mathbb{F}_q$, i.e., $\eta(g^i) = (-1)^i, \quad i = 0, 1, \ldots, q-2$. Then the *Sidel'nikov*(Lempel-Cohn-Eastman) *sequence* is defined:

$$s_n = \begin{cases} 1, & \text{if } \eta(g^n + 1) = -1, \\ 0, & \text{otherwise}, \end{cases} \qquad n = 0, 1, \ldots.$$

Definition of Legendre-Sidelnikov Sequence

- We consider the n-periodic binary sequence (s_i) :

$$s_i = \begin{cases} 1, & \text{if } (i \bmod n) \in P, \\ 0, & \text{if } (i \bmod n) \in Q^*, \\ \frac{1-\left(\frac{i}{p}\right)\eta(g^i+1)}{2}, & \text{if } (i \bmod n) \in R, \end{cases} \quad i \geq 0,$$

where p is an odd prime and q is the power of an odd prime such that $\gcd(p, q-1) = 1$.
$n = p(q-1)$,
$P = \{0, p, 2p, \ldots, (q-2)p\}$.
$Q = \left\{\frac{q-1}{2} + j(q-1) : j = 0, \ldots, p-1\right\}$,
$Q^* = Q \setminus \{\frac{n}{2}\}$ because $P \cap Q = \{\frac{n}{2}\}$,
$R = \{0, 1, 2, \ldots, n-1\} \setminus (P \cup Q^*)$.

Properties of Legendre-Sidelnikov Sequence

- This new sequence is balanced if $p = q$.
- The autocorrelation of (s_i) is given by

$$\mathrm{AC}(s_i, l) = \begin{cases} q - 1 - (p-1)((-1)^l + 1), & l \in P \setminus \{0\}, \\ (-1)^{(q-1)/2} - 1 & \\ + \left(1 - (-1)^{(q^2-1)/8}\right)\left(\frac{l}{p}\right) & \\ \left(1 + (-1)^{\frac{p-1}{2}}\right), & l \in Q^*, \\ p - q - 2 + \left(1 + (-1)^{(p-1)/2}\right)\left(\frac{l}{p}\right), & l \in R, q-1 \mid l, \\ (-1)^l - 1 + \left(\frac{l}{p}\right)(1 + (-1)^{(p-1)/2} & \\ -\eta(-g^l + 1) & \\ (1 + (-1)^{(p-1)/2+(q-1)/2+l})), & l \in R, q-1 \nmid l. \end{cases}$$

Properties of Legendre-Sidelnikov Sequence

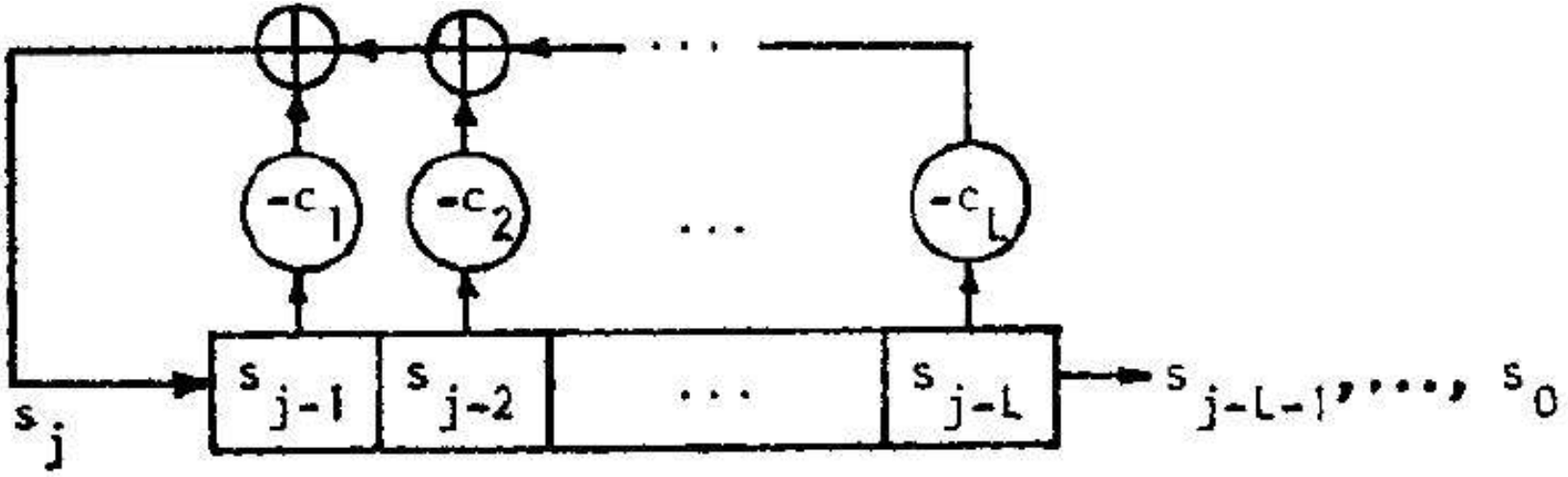
- This new sequence is balanced if $p = q$.
- The autocorrelation of (s_i) is given by

$$\mathrm{AC}(s_i, l) = \begin{cases} q - 1 - (p-1)((-1)^l + 1), & l \in P \setminus \{0\}, \\ (-1)^{(q-1)/2} - 1 & \\ + \left(1 - (-1)^{(q^2-1)/8}\right)\left(\frac{l}{p}\right) & \\ \left(1 + (-1)^{\frac{p-1}{2}}\right), & l \in Q^*, \\ p - q - 2 + \left(1 + (-1)^{(p-1)/2}\right)\left(\frac{l}{p}\right), & l \in R, q-1 \mid l, \\ (-1)^l - 1 + \left(\frac{l}{p}\right)\left(1 + (-1)^{(p-1)/2}\right. & \\ -\eta(-g^l + 1) & \\ \left.(1 + (-1)^{(p-1)/2+(q-1)/2+l})\right), & l \in R, q-1 \nmid l. \end{cases}$$

Definition of Linear Complexity

The *linear complexity* $L(S)$ over $\mathbb{F}_2$ of a binary sequence (s_i) is the shortest length L of a linear recurrence relation over $\mathbb{F}_2$

$$s_{i+L} = c_{L-1}s_{i+L-1} + \ldots + c_0 s_i, \quad 0 \leq i \leq N - L - 1.$$



On the Linear Complexity

- The linear complexity should be large enough, i. e., larger than half of the period, resisting the *Berlekamp-Massey* attack
- Algebraic expression of the linear complexity of S:

$$L(S) = N - \deg(\gcd(X^N - 1, S(X))),$$

where the **generating polynomial**
$S(X) := s_0 + s_1 X + \ldots + s_{N-1} X^{N-1}$.

On the Linear Complexity

- The linear complexity should be large enough, i. e., larger than half of the period, resisting the *Berlekamp-Massey* attack
- Algebraic expression of the linear complexity of S:

$$L(S) = N - \deg(\gcd(X^N - 1, S(X))),$$

where the **generating polynomial** $S(X) := s_0 + s_1 X + \ldots + s_{N-1} X^{N-1}$.

Linear Complexity of Other Character Sequences

- Legendre sequence (*Ding, Helleseth, Shan*)
  By using **quadratic residues and nonresidues**
- Sidelnikov sequence (*Helleseth, Yang; Kyureghyan, Pott; Meidl, Winterhof*)
  In some cases by using results on **certain cyclotomic numbers and the factorization of some cyclotomic polynomials**
- Generalized Cyclotomic binary sequence of order 2 (Ding)
  By using properties of **cyclotomic cosets**
- Two prime generators(*Brandstatter, Winterhof; Ding*);
  Two prime Sidelnikov sequence(*Brandstatter, Pirsic, Winterhof*)

Linear Complexity of Other Character Sequences

- Legendre sequence (*Ding, Helleseth, Shan*)
  By using **quadratic residues and nonresidues**
- Sidelnikov sequence (*Helleseth, Yang; Kyureghyan, Pott; Meidl, Winterhof*)
  In some cases by using results on **certain cyclotomic numbers and the factorization of some cyclotomic polynomials**
- Generalized Cyclotomic binary sequence of order 2 (Ding)
  By using properties of **cyclotomic cosets**
- Two prime generators(*Brandstatter, Winterhof; Ding*);
  Two prime Sidelnikov sequence(*Brandstatter, Pirsic, Winterhof*)

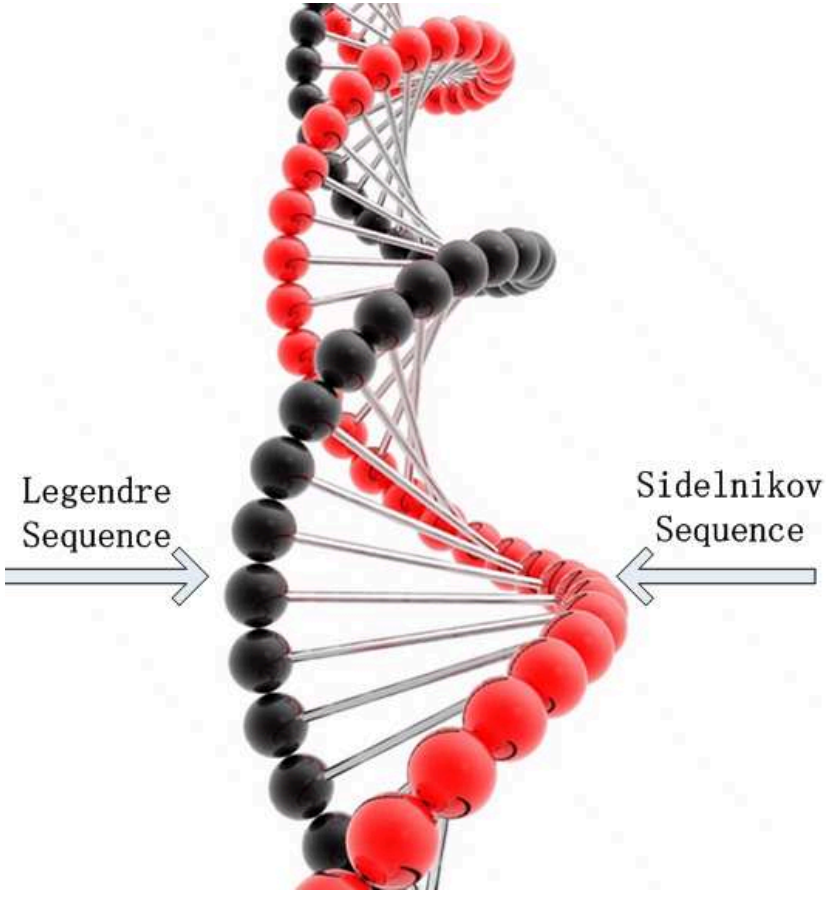
Linear Complexity of Other Character Sequences

- Legendre sequence (*Ding, Helleseth, Shan*)
  By using **quadratic residues and nonresidues**
- Sidelnikov sequence (*Helleseth, Yang; Kyureghyan, Pott; Meidl, Winterhof*)
  In some cases by using results on **certain cyclotomic numbers and the factorization of some cyclotomic polynomials**
- Generalized Cyclotomic binary sequence of order 2 (Ding)
  By using properties of **cyclotomic cosets**
- Two prime generators(*Brandstatter, Winterhof; Ding*);
  Two prime Sidelnikov sequence(*Brandstatter, Pirsic, Winterhof*)

Linear Complexity of Other Character Sequences

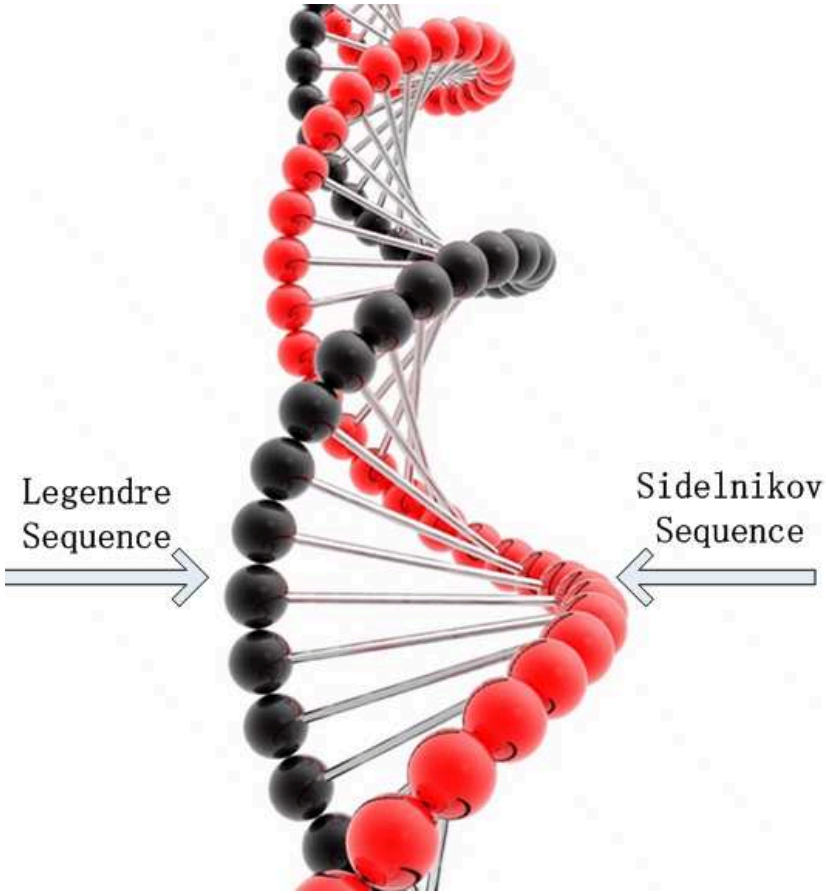
- Legendre sequence (*Ding, Helleseth, Shan*)
  By using **quadratic residues and nonresidues**
- Sidelnikov sequence (*Helleseth, Yang; Kyureghyan, Pott; Meidl, Winterhof*)
  In some cases by using results on **certain cyclotomic numbers and the factorization of some cyclotomic polynomials**
- Generalized Cyclotomic binary sequence of order 2 (Ding)
  By using properties of **cyclotomic cosets**
- Two prime generators(*Brandstatter, Winterhof; Ding*);
  Two prime Sidelnikov sequence(*Brandstatter, Pirsic, Winterhof*)

Linear Complexity of this Sequence?



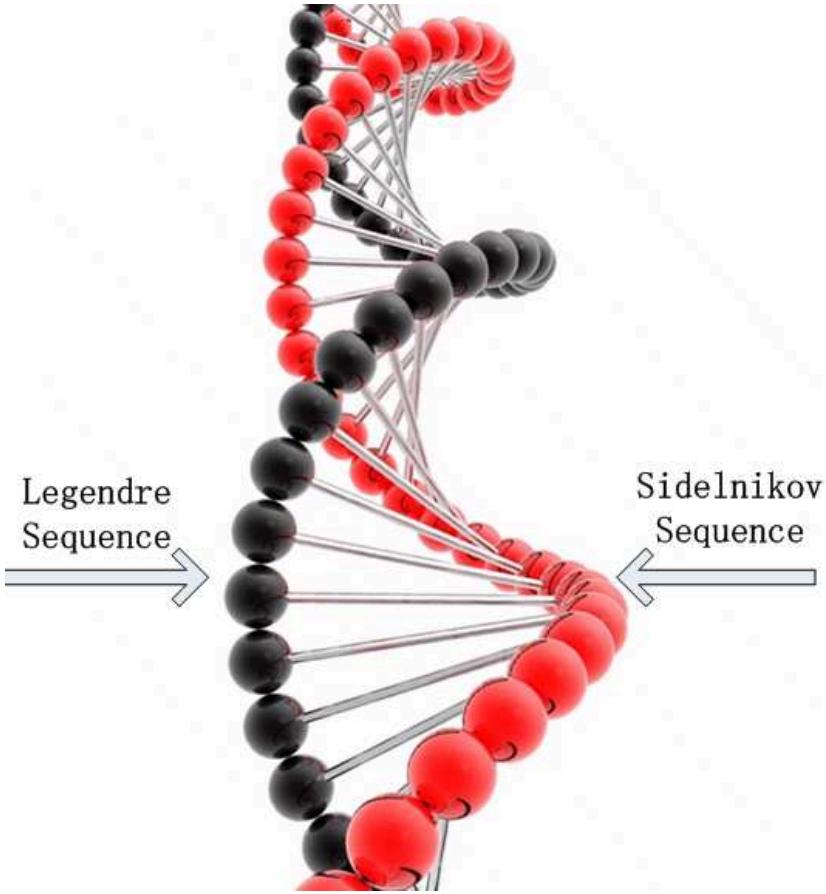
- Intuitively p (related to the Legendre sequence) and q (Sidelnikov) should both contribute 'equivalently'.
- Can we determine the exact linear complexity?

Linear Complexity of this Sequence?



- Intuitively p (related to the Legendre sequence) and q (Sidelnikov) should both contribute ‘equivalently’.
- Can we determine the exact linear complexity?

Linear Complexity of this Sequence?



- Intuitively p (related to the Legendre sequence) and q (Sidelnikov) should both contribute ‘equivalently’.
- Can we determine the exact linear complexity?

Generating Polynomial of Legendre-Sidelnikov Sequence

Note that

$$X^n - 1 = (X^{rp} - 1)^2,$$

where $r = \frac{q-1}{2}$.

Next we discuss the multiplicities of 1, β(rth root of unity), α(pth root of unity), and other prth roots of unity for $S(X)$.

Generating Polynomial of Legendre-Sidelnikov Sequence

Note that

$$X^n - 1 = (X^{rp} - 1)^2,$$

where $r = \frac{q-1}{2}$.
Next we discuss the multiplicities of 1, β(rth root of unity), α(pth root of unity), and other prth roots of unity for $S(X)$.

On the multiplicity of 1

Lemma A

If $p \equiv 1 \pmod 4$, then for $k \geq 1$ satisfying $2^t - 1 \leq k < 2^{t+1} - 1$ with some positive integer t, we have $S^{(j)}(1) = 0$ for all $j \leq k$ if and only if $q \equiv 1 \pmod{2^{t+1}}$. Equivalently, if $p \equiv 3 \pmod 4$, 1 is not a root of $S(X)$; if $p \equiv 1 \pmod 4$, and $q \equiv 1 \pmod{2^l}$ for the maximal integer l, the multiplicity of the root 1 is $2^l - 1$.

Proof: Suppose the conclusion is true for $2^t - 1 \leq k < 2^{t+1} - 1$ on some t. Then for $k = 2^{t+1} - 1$, by Lucas property and Hasse derivative

$$S^{(k)}(1) = \sum_{i=0}^{p(q-1)-1} \binom{i}{k} s_i = \sum_{\substack{i=0 \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}}^{p(q-1)-1} s_i$$

$$= \sum_{\substack{i \in P \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}} s_i + \sum_{\substack{i \in \mathbb{Z}_n \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}} \left(\frac{i}{p}\right) \eta(g^i + 1).$$

On the multiplicity of 1

Lemma A

If $p \equiv 1 \pmod 4$, then for $k \geq 1$ satisfying $2^t - 1 \leq k < 2^{t+1} - 1$ with some positive integer t, we have $S^{(j)}(1) = 0$ for all $j \leq k$ if and only if $q \equiv 1 \pmod{2^{t+1}}$. Equivalently, if $p \equiv 3 \pmod 4$, 1 is not a root of $S(X)$; if $p \equiv 1 \pmod 4$, and $q \equiv 1 \pmod{2^l}$ for the maximal integer l, the multiplicity of the root 1 is $2^l - 1$.

Proof: Suppose the conclusion is true for $2^t - 1 \leq k < 2^{t+1} - 1$ on some t. Then for $k = 2^{t+1} - 1$, by Lucas property and Hasse derivative

$$S^{(k)}(1) = \sum_{i=0}^{p(q-1)-1} \binom{i}{k} s_i = \sum_{\substack{i=0 \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}}^{p(q-1)-1} s_i$$

$$= \sum_{\substack{i \in P \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}} s_i + \sum_{\substack{i \in \mathbb{Z}_n \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}} \left(\frac{i}{p}\right) \eta(g^i + 1).$$

On the multiplicity of 1

From $q \equiv 1 \pmod{2^{t+1}}$ we derive

$$\sum_{\substack{i \in P \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}} s_i = \frac{q-1}{2^{t+1}},$$

and

$$\sum_{\substack{i \in \mathbb{Z}_n \\ i \equiv 2^{t+1}-1 \pmod{2^{t+1}}}} \left(\frac{i}{p}\right) \eta(g^i + 1) = \sum_{i \in \mathbb{Z}_p} \left(\frac{i}{p}\right) \cdot \sum_{\substack{i \equiv 2^{t+1}-1 \pmod{2^{t+1}} \\ i \in Z_{q-1}}} \eta(g^i + 1) = 0.$$

Hence we have

$$S^{(k)}(1) = \begin{cases} 0 & q \equiv 1 \pmod{2^{t+2}} \\ 1 & q \equiv 1 + 2^{t+1} \pmod{2^{t+2}}. \end{cases}$$

For the other cases $2^{t+1} - 1 < k < 2^{t+2} - 1$ analogously.

On the multiplicity of β

Lemma B

Let $q-1=2r$ with an integer divisor r. For each rth root of unity $\beta \neq 1$, if $p \equiv 3 \pmod 4$ we have $S(\beta) \neq 0$; if $p \equiv 1 \pmod 4$ we have $S(\beta) = 0$.

Proof: We have

$$S(\beta) = \sum_{h=0}^{r-1} \sum_{j=0}^{2p-1} s_{h+jr} \beta^h.$$

Since $h + jr \notin Q^*$ for $h \neq 0$, and for $i \in R$ $(-1)^{s_i} = \left(\frac{i}{p}\right) \eta(g^i + 1)$, we have

$$(-1)^{\sum_{j=0}^{2p-1} s_{h+jr}} = (-1)^{|j:h+jr \in P|} \prod_{\substack{j=0 \\ h+jr \notin P}}^{2p-1} \left(\frac{h+jr}{p}\right) \eta((-1)^j g^h + 1).$$

On the multiplicity of β-Continued

By the property of Legendre symbol and quadratic character, the coefficients of β^h is 0 over $\mathbb{F}_2$ for $h = 1, \ldots, r-1$, and that of β^0 is $(-1)^{\frac{p-1}{2}}$. □

Lemma C

Let $q - 1 = 2r$ with an integer divisor r. For each rth root of unity $\beta \neq 1$, if $p \equiv 1 \pmod 4$ we have $S^{(1)}(\beta) = 0$.

On the multiplicity of β-Continued

By the property of Legendre symbol and quadratic character, the coefficients of β^h is 0 over $\mathbb{F}_2$ for $h = 1, \ldots, r-1$, and that of β^0 is $(-1)^{\frac{p-1}{2}}$. □

Lemma C

Let $q-1 = 2r$ with an integer divisor r. For each rth root of unity $\beta \neq 1$, if $p \equiv 1 \pmod 4$ we have $S^{(1)}(\beta) = 0$.

On the multiplicity of α

Lemma D

Let $\alpha \neq 1$ be a pth root of unity. If $p \equiv \pm 3 \pmod 8$, then $S(\alpha) \neq 0$; if $p \equiv \pm 1 \pmod 8$, then one half of the pth roots of unity satisfy $S(\alpha) = 0$ and the other half of roots satisfy $S(\alpha) \neq 0$.

By the property of (non)quadratic residue squares and cyclotomic number.

Lemma E

Let $p \equiv \pm 1 \pmod 8$. For the half of the pth roots of unity $\alpha \neq 1$ satisfying $S(\alpha) = 0$, we also have $S^{(1)}(\alpha) = 0$ if $q \equiv 7 \pmod 8$, and $S^{(1)}(\alpha) \neq 0$ if $q \equiv 3 \pmod 8$.

On the multiplicity of α

Lemma D

Let $\alpha \neq 1$ be a pth root of unity. If $p \equiv \pm 3 \pmod 8$, then $S(\alpha) \neq 0$; if $p \equiv \pm 1 \pmod 8$, then one half of the pth roots of unity satisfy $S(\alpha) = 0$ and the other half of roots satisfy $S(\alpha) \neq 0$.

By the property of (non)quadratic residue squares and cyclotomic number.

Lemma E

Let $p \equiv \pm 1 \pmod 8$. For the half of the pth roots of unity $\alpha \neq 1$ satisfying $S(\alpha) = 0$, we also have $S^{(1)}(\alpha) = 0$ if $q \equiv 7 \pmod 8$, and $S^{(1)}(\alpha) \neq 0$ if $q \equiv 3 \pmod 8$.

Factorization of the Generating Polynomial of Legendre-Sidelnikov Sequence

We require a simple factorization for $x^n - 1$ so that it is possible to determine the linear complexity of the Legendre-Sidelnikov sequence.
Now we restrict q to a safe prime, then

$$X^n - 1 = (X^{rp} - 1)^2 = \Big((X-1)\Phi_r(X)\Phi_p(X)\Phi_{rp}(X)\Big)^2.$$

Let γ be a primitive rpth root of unity. Next we need to investigate the multiplicity of γ, which is the most difficult and crucial part for determining the exact linear complexity.

On the multiplicity of γ

Lemma F

Let $q = 2r + 1$ be a safe prime, $r \neq 3$, where 2 is a primitive root modulo r. Then we have $S(\gamma) \neq 0$.

Proof: Note that $S(\gamma) = \sum_{i=0}^{rp-1}(s_i + s_{i+rp})\gamma^i$. For our case we have

$$s_i + s_{i+rp} = \begin{cases} 0, & i \in P \\ 1 - \frac{\eta(g^i+1)+\eta(-g^i+1)}{2}, & i \in R, i + rp \in R \\ \frac{1-\left(\frac{i}{p}\right)\eta(2)}{2}, & i \in Q^*, i + rp \in R \\ \frac{1-\left(\frac{i}{p}\right)\eta(2)}{2}, & i \in R, i + rp \in Q^*. \end{cases}$$

On the multiplicity of γ

Lemma F

Let $q = 2r + 1$ be a safe prime, $r \neq 3$, where 2 is a primitive root modulo r. Then we have $S(\gamma) \neq 0$.

Proof: Note that $S(\gamma) = \sum_{i=0}^{rp-1}(s_i + s_{i+rp})\gamma^i$. For our case we have

$$s_i + s_{i+rp} = \begin{cases} 0, & i \in P \\ 1 - \frac{\eta(g^i+1)+\eta(-g^i+1)}{2}, & i \in R, i + rp \in R \\ \frac{1-\left(\frac{i}{p}\right)\eta(2)}{2}, & i \in Q^*, i + rp \in R \\ \frac{1-\left(\frac{i}{p}\right)\eta(2)}{2}, & i \in R, i + rp \in Q^*. \end{cases}$$

Proof-continued

Note that γ can be expressed as $\gamma_1\gamma_2$, where γ_1 is a primitive rth root of unity, and γ_2 is a primitive pth root of unity.

$$
\begin{aligned}
S(\gamma) &= \sum_{i=0}^{rp-1}(s_i + s_{i+rp} - 1)\gamma^i \\
&= \sum_{\substack{i=0 \\ i\in R, i+rp\in R}}^{rp-1} \frac{\eta(g^i+1)+\eta(-g^i+1)}{2}\gamma_1^i\gamma_2^i + \sum_{\substack{i=0 \\ i\in P}}^{rp-1}\gamma_1^i\gamma_2^i \\
&+ \sum_{\substack{i=0 \\ i\in Q^*, i+rp\in R}}^{rp-1} \frac{1+\left(\frac{i}{p}\right)\eta(2)}{2}\gamma_1^i\gamma_2^i + \sum_{\substack{i=0 \\ i\in R, i+rp\in Q^*}}^{rp-1} \frac{1+\left(\frac{i}{p}\right)\eta(2)}{2}\gamma_1^i\gamma_2^i.
\end{aligned}
$$

Proof -Continued

Then we obtain

$$S(\gamma) = \sum_{i \in \mathbb{Z}_p^*} \frac{1 + \left(\frac{i}{p}\right)\eta(2)}{2}\gamma_2^i + \sum_{i=1}^{r-1} \frac{1 + \eta(1 - g^{2i})}{2}\gamma_1^i.$$

Finally we have $S(\gamma) \notin \mathbb{F}_4$ and the conclusion follows. □

Result on the Linear Complexity-Theorem 1

Theorem 1

The linear complexity of Legendre-Sidelnikov sequences $L(S)$ satisfies:

$$\begin{cases} p-1 \\ 2p+q-3 \\ 2(p-1) \\ p+q-2 \end{cases} \leq L(S) \leq \begin{cases} p(q-1)-\frac{p+2q-5}{2} & p \equiv 1 \bmod 8 \\ p(q-1) & p \equiv 3 \bmod 8 \\ p(q-1)-q+2 & p \equiv 5 \bmod 8 \\ p(q-1)-\frac{p-1}{2} & p \equiv 7 \bmod 8 \end{cases}$$

Experiments

Table: The Linear Complexity of Legendre-Sidelnikov Sequences

	p	q	g	*LinearComplexity*	*GivenUpperBound*
$p \equiv 1 \bmod 8$	17	19	2	**281**	**281**
	41	37	2	1381	1421
$p \equiv 3 \bmod 8$	19	29	2	**532**	**532**
	43	43	3	1722	1806
$p \equiv 5 \bmod 8$	13	17	3	**193**	**193**
	37	41	7	1369	1441
$p \equiv 7 \bmod 8$	23	29	2	**633**	**633**
	31	37	2	1071	1101

The upper bounds listed in Theorem 1 can be attained as shown in Table. The gap between listed lower bounds and upper bounds remains an open problem.

Result on the Linear Complexity-Theorem 2

Theorem 2

Let $q = 2r + 1$ be a safe prime, $r \neq 3$, where 2 is a primitive root modulo r. If $p \equiv 3 \pmod 8$, then the linear complexity of Legendre-Sidelnikov sequences is $L(S) = p(q-1)$; $L(S) = p(q-1) - p + 1$ if $p \equiv q \equiv 7 \pmod 8$, and $L(S) = p(q-1) - \frac{p-1}{2}$ if $p \equiv 7 \pmod 8, q \equiv 3 \pmod 8$.

Note that $X^{rp} - 1 = (X-1)\Phi_r(X)\Phi_p(X)\Phi_{rp}(X)$.

Result on the Linear Complexity-Theorem 2

Theorem 2

Let $q = 2r + 1$ be a safe prime, $r \neq 3$, where 2 is a primitive root modulo r. If $p \equiv 3 \pmod 8$, then the linear complexity of Legendre-Sidelnikov sequences is $L(S) = p(q-1)$; $L(S) = p(q-1) - p + 1$ if $p \equiv q \equiv 7 \pmod 8$, and $L(S) = p(q-1) - \frac{p-1}{2}$ if $p \equiv 7 \pmod 8, q \equiv 3 \pmod 8$.

Note that $X^{rp} - 1 = (X-1)\Phi_r(X)\Phi_p(X)\Phi_{rp}(X)$.

Result on the Linear Complexity-Theorem 3

Theorem 3

If $q = 2^s + 1$ is a Fermat prime, then the linear complexity of Legendre-Sidelnikov sequences is $L(S) = p(q-1)$ if $p \equiv 3 \pmod 8$, and $L(S) = p(q-1) - q + 2$ if $p \equiv 5 \pmod 8$.

Note that

$$1 - X^n = (1 - X^p)^{2^s} = \Big((1 - X)(1 + X + \cdots + X^{p-1})\Big)^{q-1}.$$

Result on the Linear Complexity-Theorem 3

Theorem 3

If $q = 2^s + 1$ is a Fermat prime, then the linear complexity of Legendre-Sidelnikov sequences is $L(S) = p(q-1)$ if $p \equiv 3 \pmod 8$, and $L(S) = p(q-1) - q + 2$ if $p \equiv 5 \pmod 8$.

Note that

$$1 - X^n = (1 - X^p)^{2^s} = \left((1 - X)(1 + X + \cdots + X^{p-1})\right)^{q-1}.$$

Result on the Linear Complexity-Choosing Parameters

If $p = q = 2r + 1 \equiv 3 \pmod 8$ are both safe primes, and 2 is a primitive root modulo r, the linear complexity is just the period. For example, $11, 59, 107, \ldots, 587, 1019, 1307, \ldots$. And if $p = q = 2r + 1 \equiv 7 \pmod 8$ are both safe primes, and 2 is a primitive root modulo r, then the linear complexity of Legendre-Sidelnikov sequences is $(p-1)^2$. Similarly, $23, 167, \ldots$.

Conjecture: We may remove the condition of 2 being a primitive root modulo r; and determine the exact linear complexity value for more cases.

Result on the Linear Complexity-Choosing Parameters

If $p = q = 2r + 1 \equiv 3 \pmod 8$ are both safe primes, and 2 is a primitive root modulo r, the linear complexity is just the period. For example, $11, 59, 107, \ldots, 587, 1019, 1307, \ldots$. And if $p = q = 2r + 1 \equiv 7 \pmod 8$ are both safe primes, and 2 is a primitive root modulo r, then the linear complexity of Legendre-Sidelnikov sequences is $(p-1)^2$. Similarly, $23, 167, \ldots$.

Conjecture: We may remove the condition of 2 being a primitive root modulo r; and determine the exact linear complexity value for more cases.

References

- Ding C., Helleseth T., Shan W.: On the linear complexity of Legendre sequences. IEEE Trans. Inf. Theory, **44**(3), 1276 - 1278, (1998).
- Helleseth T., Yang K.: On binary sequences with period $n = p^m - 1$ with optimal autocorrelation. In: SETA 2001, LNCS, Helleseth T., Kumar P., Yang K., eds. pp. 209 - 217, Springer, (2002).
- Jungnickel D.: Finite Fields. BI-Wissenschaftsverlag, Mannheim, (1993).
- Kyureghyan G. M., Pott A.: On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences. Des. Codes Cryptogr., **29**, 149 - 164, (2003).
- Lidl R., Niederreiter H.: Finite Fields. Addison-Wesley, Reading, MA, (1983).
- Meidl W., Winterhof A.: Some notes on the linear complexity of Sidel'nikov-Lempel-Cohn-Eastman sequences. Des. Codes Cryptogr., **38**(2), 159 - 178, (2006).
- Su M.: On the Linear Complexity of Legendre-Sidelnikov Sequences, Designs, Codes and Cryptography, Springer published online, 10.1007/s10623-013-9889-1, (2013).
- Su M., Winterhof A.: Autocorrelation of Legendre-Sidelnikov sequences. IEEE Trans. Inf. Theory, **56**, 1714-1718, (2010).
- Topuzoğlu A., Winterhof A.: Pseudorandom sequences. Topics in geometry, coding theory and cryptography, Algebr. Appl., 6, Springer, Dordrecht, 135-166, (2007).

Thank you !
vielen Dank!

nksuker@gmail.com