Journal of Complexity 24 (2008) 648–659

Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

On the linear complexity of Sidel'nikov sequences over nonprime fields

Nina Brandstätter [a], Wilfried Meidl [b,*]

[a] *Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040 Linz, Austria*

[b] *Sabancı University, MDBF, Orhanlı, 34956 Tuzla, İstanbul, Turkey*

ARTICLE INFO

Article history:
Received 19 September 2007
Accepted 23 April 2008
Available online 20 May 2008

Keywords:
Sidel'nikov sequence
Linear complexity
Cyclotomic numbers
Sequences over finite fields

ABSTRACT

We introduce a generalization of Sidel'nikov sequences for arbitrary finite fields. We show that several classes of Sidel'nikov sequences over arbitrary finite fields exhibit a large linear complexity. For Sidel'nikov sequences over $\mathbb{F}_8$ we provide exact values for their linear complexity.

1. Introduction

For a prime power q let $\mathbb{F}_q$ be the finite field of order q and let d be a positive divisor of $q-1$. The *cyclotomic classes of order d* give a partition of $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ defined by

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

for a primitive element α of $\mathbb{F}_q$.
For a prime divisor d of $q-1$, Sidel'nikov [24] introduced the $(q-1)$-periodic sequence $S = s_0, s_1, \ldots$ with terms in the finite field $\mathbb{F}_d$ (we will also write over the finite field $\mathbb{F}_d$) defined by

$$\begin{aligned} &s_n = j \iff \alpha^n + 1 \in D_j, \quad n = 0, \ldots, q-2, \ n \ne (q-1)/2, \\ &s_{(q-1)/2} = 0, \quad \text{and} \\ &s_{n+q-1} = s_n, \quad n \ge 0. \end{aligned} \tag{1}$$

Independently in [16] Lempel, Cohn and Eastman studied the sequence (1) for $d = 2$.

* Corresponding author.
E-mail address: wmeidl@sabanciuniv.edu (W. Meidl).

0885-064X/$ – see front matter
doi:10.1016/j.jco.2008.04.002

In the following we suggest a natural generalization of the sequence (1) for arbitrary finite fields. Suppose that the divisor $d = p^t$ of $q-1$ is a power of the prime p and let $\{\beta_0, \beta_1, \ldots, \beta_{t-1}\}$ be a basis of $\mathbb{F}_{p^t}$ over $\mathbb{F}_p$. Then we define the Sidel'nikov sequence $S = s_0, s_1, \ldots$ with period $q-1$ and terms in the finite field $\mathbb{F}_{p^t}$ by

$$\begin{aligned} &s_n = \xi_j \Longleftrightarrow \alpha^n + 1 \in D_j, \quad n = 0, \ldots, q-2, n \neq (q-1)/2, \\ &s_{(q-1)/2} = 0, \quad \text{and} \\ &s_{n+q-1} = s_n, \quad n \geq 0, \end{aligned} \tag{2}$$

where $\xi_j = j_0\beta_0 + j_1\beta_1 + \cdots + j_{t-1}\beta_{r-1}$ if $(j_0, j_1, \ldots, j_{t-1})_p$ is the p-ary representation of the integer j. We remark that the exact appearance of the Sidel'nikov sequence depends on the choice of the basis.

The *linear complexity* of an N-periodic sequence $S = s_0, s_1, \ldots$ over a finite field $\mathbb{F}_d$, denoted by $L(S)$, is the smallest nonnegative integer L for which there exist coefficients $c_1, c_2, \ldots, c_L \in \mathbb{F}_d$ such that

$$s_n + c_1 s_{n-1} + \cdots + c_L s_{n-L} = 0 \quad \text{for all } n \geq L.$$

The linear complexity is of fundamental importance as a complexity measure for periodic sequences used as a keystream for a stream cipher in cryptography (see [20–23]).

The linear complexity of the binary Sidel'nikov sequence has been investigated in [13,15,19]. For results on the linear complexity of the Sidel'nikov sequence defined by (1) for an arbitrary prime divisor d of $q-1$ we can refer to [4].

Since the finite field $\mathbb{F}_q$, $q = u^m$, plays an important role in the construction of the Sidel'nikov sequence S given by (1), it is also reasonable to interpret S as a sequence over the prime field $\mathbb{F}_u$. Results on the linear complexity of this sequence can be found in [7,8,11,12] if $d = 2$, and in [2,5,14] for arbitrary divisors d of $q-1$ (in this case d need not necessarily be a prime).

In this article we investigate the linear complexity of the generalization (2) of the Sidel'nikov sequence for arbitrary finite fields. After recalling some basic facts and techniques in Section 2, in Section 3 we establish good lower bounds on the linear complexity for several classes of sequences of the form (2). In Section 4 we present exact values for the linear complexity of Sidel'nikov sequences over $\mathbb{F}_8$.

2. Preliminaries

Let $d = p^t$ be a power of the prime p and let $S = s_0, s_1, \ldots$ be an N-periodic sequence over the finite field $\mathbb{F}_d$. Then we can identify S with the polynomial $S(X) := s_0 + s_1 X + \cdots + s_{N-1}X^{N-1} \in \mathbb{F}_d[X]$ of degree at most $N-1$. The linear complexity $L(S)$ of the sequence S is then given by (cf. [6, Lemma 8.2.1])

$$L(S) = N - \deg(\gcd(X^N - 1, S(X))). \tag{3}$$

If $N = p^s r$ with $\gcd(p, r) = 1$, then we have $X^N - 1 = (X^r - 1)^{p^s}$. Consequently, in order to calculate the linear complexity of S we are interested in the multiplicities of the rth roots of unity as roots of the polynomial $S(X)$. The multiplicity of roots of the polynomial $S(X)$ can be determined with the kth *Hasse derivative* (cf. [10]) $S(X)^{(k)}$ of $S(X)$, which is defined by

$$S(X)^{(k)} = \sum_{n=k}^{N-1} \binom{n}{k} s_n X^{n-k}.$$

The multiplicity of γ as a root of $S(X)$ is v if $S(\gamma) = S(\gamma)^{(1)} = \cdots = S(\gamma)^{(v-1)} = 0$ and $S(\gamma)^{(v)} \neq 0$ (cf. [17, Lemma 6.51]).

Consequently we are interested in the Hasse derivatives of the polynomial $S(X)$ which corresponds to the sequence (2):

The binomial coefficients modulo p appearing in $S(X)^{(k)}$ can be evaluated with *Lucas' congruence* (cf. [9,18])

$$\binom{n}{k} \equiv \binom{n_0}{k_0} \cdots \binom{n_c}{k_c} \mod p,$$