Finite Fields and Their Applications ••• (••••) •••–•••

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences

Wilfried Meidl [a], Ferruh Özbudak [b,*]

[a] *Faculty of Engineering and Natural Sciences, Sabancı University, Tuzla, 34956, İstanbul, Turkey*
[b] *Department of Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey*

ARTICLE INFO

Article history:
Received 7 August 2008
Revised 25 September 2008

Communicated by Gary L. Mullen

Keywords:
Joint linear complexity
Generalized joint linear complexity
Multisequences
Linear recurring sequences

ABSTRACT

Since the $\mathbb{F}_q$-linear spaces $\mathbb{F}_q^m$ and $\mathbb{F}_{q^m}$ are isomorphic, an m-fold multisequence $\boldsymbol{S}$ over the finite field $\mathbb{F}_q$ with a given characteristic polynomial $f \in \mathbb{F}_q[x]$, can be identified with a single sequence $\mathcal{S}$ over $\mathbb{F}_{q^m}$ with characteristic polynomial f. The linear complexity of $\mathcal{S}$, which will be called the generalized joint linear complexity of $\boldsymbol{S}$, can be significantly smaller than the conventional joint linear complexity of $\boldsymbol{S}$. We determine the expected value and the variance of the generalized joint linear complexity of a random m-fold multisequence $\boldsymbol{S}$ with given minimal polynomial. The result on the expected value generalizes a previous result on periodic m-fold multisequences. Moreover we determine the expected drop of linear complexity of a random m-fold multisequence with given characteristic polynomial f, when one switches from conventional joint linear complexity to generalized joint linear complexity.

1. Introduction

A sequence $S = s_0, s_1, \ldots$ with terms in a finite field $\mathbb{F}_q$ with q elements (or over the finite field $\mathbb{F}_q$) is called a *linear recurring sequence* over $\mathbb{F}_q$ with *characteristic polynomial*

$$f(x) = \sum_{i=0}^{l} c_i x^i \in \mathbb{F}_q[x]$$

* Corresponding author.
E-mail addresses: wmeidl@sabanciuniv.edu (W. Meidl), ozbudak@metu.edu.tr (F. Özbudak).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2008.09.004

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

of degree l, if

$$\sum_{i=0}^{l} c_i s_{n+i} = 0 \quad \text{for } n = 0, 1, \ldots.$$

Without loss of generality we can always assume that $f(x)$ is monic, i.e. $c_l = 1$. In accordance with the notation in [2] we denote the set of sequences over $\mathbb{F}_q$ with characteristic polynomial f by $\mathcal{M}_q^{(1)}(f)$. The *minimal polynomial* of a linear recurring sequence $S \in \mathcal{M}_q^{(1)}(f)$ is defined to be the (uniquely determined) monic polynomial $d(x) \in \mathbb{F}_q[x]$ of smallest degree such that $S \in \mathcal{M}_q^{(1)}(d)$. We remark that then d is a divisor of f. The degree of d is called the *linear complexity* $L(S)$ of the sequence S.

Motivated by the study of vectorized stream cipher systems (see [1,3]) we consider the set of m parallel sequences over $\mathbb{F}_q$, each of them being in $\mathcal{M}_q^{(1)}(f)$. As usual we call this set the set of *m-fold multisequences* over $\mathbb{F}_q$ with joint characteristic polynomial f and denote it by $\mathcal{M}_q^{(m)}(f)$. The *joint minimal polynomial* of an m-fold multisequence $\boldsymbol{S} = (\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathcal{M}_q^{(m)}(f)$ is then defined to be the (uniquely determined) monic polynomial d of least degree which is a characteristic polynomial for all sequences σ_r, $1 \leqslant r \leqslant m$. The *joint linear complexity* $L_q^{(m)}(\boldsymbol{S})$ of $\boldsymbol{S}$ is then the degree of d.

Let $\boldsymbol{S} = (\sigma_1, \sigma_2, \ldots, \sigma_m) \in \mathcal{M}_q^{(m)}(f)$ and suppose that $\sigma_r = s_{r,0}s_{r,1}s_{r,2}\ldots$, $1 \leqslant r \leqslant m$. Then there exist unique polynomials $g_r \in \mathbb{F}_q[x]$ with $\deg(g_r) < \deg(f)$ and $g_r/f = s_{r,0} + s_{r,1}x + s_{r,2}x^2 \cdots$, $1 \leqslant r \leqslant m$. By [7, Lemma 1] this describes a one-to-one correspondence between the set $\mathcal{M}_q^{(m)}(f)$ and the set of m-tuples of the form $(g_1/f, g_2/f, \ldots, g_m/f)$, $g_r \in \mathbb{F}_q[x]$ and $\deg(g_r) < \deg(f)$ for $1 \leqslant r \leqslant m$.

If $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ corresponds to $(g_1/f, g_2/f, \ldots, g_m/f)$, then the joint minimal polynomial d of $\boldsymbol{S}$ is the unique polynomial in $\mathbb{F}_q[x]$ for which there exist $h_1, \ldots, h_m \in \mathbb{F}_q[x]$ with $g_r/f = h_r/d$ for $1 \leqslant r \leqslant m$, and $\gcd(h_1, \ldots, h_m, d) = 1$. Therefore the joint linear complexity of $\boldsymbol{S}$ is then given by

$$L_q^{(m)}(\boldsymbol{S}) = \deg(f) - \deg\big(\gcd(g_1, g_2, \ldots, g_m, f)\big).$$

Since the $\mathbb{F}_q$-linear spaces $\mathbb{F}_q^m$ and $\mathbb{F}_{q^m}$ are isomorphic, the multisequence $\boldsymbol{S}$ can be identified with a single sequence $\mathcal{S}$ having its terms in the extension field $\mathbb{F}_{q^m}$, namely $\mathcal{S} = \mathcal{S}(\boldsymbol{S}, \boldsymbol{\xi}) = s_0, s_1, \ldots$ with

$$s_n = \xi_1 s_{1,n} + \cdots + \xi_m s_{m,n} \in \mathbb{F}_{q^m}, \quad n \geqslant 0, \tag{1.1}$$

where $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ is an arbitrary but fixed ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. This describes a one-to-one correspondence between the sets $\mathcal{M}_q^{(m)}(f)$ and $\mathcal{M}_{q^m}^{(1)}(f)$.

Let $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ correspond to $(g_1/f, g_2/f, \ldots, g_m/f)$, then it is easily seen that the single sequence $\mathcal{S} \in \mathcal{M}_{q^m}^{(1)}(f)$ defined as in (1.1) corresponds to the 1-tuple (G/f) with

$$G(x) = g_1\xi_1 + g_2\xi_2 + \cdots + g_m\xi_m.$$

The minimal polynomial of $\mathcal{S}$ is then $d = f/\gcd(G, f) \in \mathbb{F}_{q^m}[x]$ and the linear complexity of the sequence $\mathcal{S}$, which we will call the *generalized joint linear complexity* of $\boldsymbol{S}$ and denote by $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$, is given by

$$L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) = \deg(f) - \deg\big(\gcd(G, f)\big),$$

where the greatest common divisor is now calculated in $\mathbb{F}_{q^m}[x]$. The dependence of the generalized joint linear complexity $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ on the ordered basis $\boldsymbol{\xi}$ follows from the definition (cf. [5, Example 3]).

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

Clearly we always have $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) \leqslant L_q^{(m)}(\boldsymbol{S})$, in some cases $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})$ can be considerably smaller than $L_q^{(m)}(\boldsymbol{S})$. However in [5, Theorem 2] it has been pointed out that

$$L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) \geqslant \sum_{i=1}^{k} a_i \frac{\deg(r_i)}{\gcd(\deg(r_i), m)}$$

if $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$, $f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$ is the canonical factorization of f into irreducibles over $\mathbb{F}_q$, and the joint minimal polynomial of $\boldsymbol{S}$ is $d = r_1^{a_1} r_2^{a_2} \cdots r_k^{a_k}$, $0 \leqslant a_i \leqslant e_i$ for $1 \leqslant i \leqslant k$. As one consequence we will always have $L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S}) = L_q^{(m)}(\boldsymbol{S})$ if $\gcd(\deg(r_i), m) = 1$ for $i = 1, 2, \ldots, k$ (cf. [5, Theorem 1]). In [4, Theorem 3] the expected value for the generalized joint linear complexity of a random m-fold multisequence $\boldsymbol{S}$ with minimal polynomial $x^N - 1$ for a given integer N has been determined. In this article with a different method we obtain much more general results and present expected value and variance for the generalized joint linear complexity of a random m-fold multisequence $\boldsymbol{S}$ with an arbitrary given minimal polynomial. Moreover we present results on the expected value of $D(\boldsymbol{S}) := \frac{L_q^{(m)}(\boldsymbol{S}) - L_{q^m,\boldsymbol{\xi}}(\boldsymbol{S})}{L_q^{(m)}(\boldsymbol{S})}$, the difference of joint linear complexity and generalized joint linear complexity in relation to the value for the joint linear complexity of an m-fold multisequence $\boldsymbol{S}$, which estimates the expected drop of linear complexity if one switches from conventional joint linear complexity to generalized joint linear complexity.

The rest of the paper is organized as follows. In Section 2 we fix some notation and we give some basic results that we use later. We obtain our main results in Section 3.

2. Preliminaries

We first recall an important function on the set of monic polynomials in $\mathbb{F}_q[x]$ and some of its properties (see [2, Section 2]). For a monic polynomial $f \in \mathbb{F}_q[x]$ and a positive integer m we let $\Phi_q^{(m)}(f)$ denote the number of m-fold multisequences over $\mathbb{F}_q$ with joint minimal polynomial f. Then we have [2, Lemmas 2.1 and 2.2]

$$\sum_{d|f} \Phi_q^{(m)}(d) = q^{m \deg(f)}, \tag{2.1}$$

$$\Phi_q^{(m)}(f_1 f_2) = \Phi_q^{(m)}(f_1)\Phi_q^{(m)}(f_2) \quad \text{if } \gcd(f_1, f_2) = 1. \tag{2.2}$$

Let $\mathcal{N}_q^{(m)}(f)$ denote the subset of $\mathcal{M}_q^{(m)}(f)$ consisting of multisequences $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ such that $L_q^{(m)}(\boldsymbol{S}) = \deg(f)$. It is clear that

$$\left|\mathcal{N}_q^{(m)}(f)\right| = \Phi_q^{(m)}(f).$$

For an ordered basis $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ let $\widehat{\mathcal{N}}_{q^m,\boldsymbol{\xi}}^{(1)}(f)$ be the subset of $\mathcal{M}_{q^m}^{(1)}(f)$ given by

$$\widehat{\mathcal{N}}_{q^m,\boldsymbol{\xi}}^{(1)}(f) = \left\{\mathcal{S} = \mathcal{S}(\boldsymbol{S}, \boldsymbol{\xi}) \colon\ \boldsymbol{S} \in \mathcal{N}_q^{(m)}(f)\right\}.$$

It is obvious that $|\widehat{\mathcal{N}}_{q^m,\boldsymbol{\xi}}^{(1)}(f)| = |\mathcal{N}_q^{(m)}(f)| = \Phi_q^{(m)}(f)$.

Proposition 2.1. *Let $f \in \mathbb{F}_q[x]$ be a monic polynomial with $\deg(f) \geqslant 1$ and suppose that*

$$f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$$

is the canonical factorization of f into irreducibles over $\mathbb{F}_q$. Let $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_m)$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, let $\mathcal{S}$ be a sequence in $\mathcal{M}^{(1)}_{q^m}(f)$ and let $d \in \mathbb{F}_{q^m}[x]$ be its minimal polynomial. Then $\mathcal{S} \in \widehat{\mathcal{N}}^{(1)}_{q^m,\boldsymbol{\xi}}(f)$ if and only if d is of the form

$$d = d_1 d_2 \cdots d_k,$$

where $d_1, d_2, \ldots, d_k \in \mathbb{F}_{q^m}[x]$ and $d_1 \mid r_1^{e_1}$, $d_2 \mid r_2^{e_2}$, $\ldots$, $d_k \mid r_k^{e_k}$, and

$$d_1 \nmid r_1^{e_1-1}, \quad d_2 \nmid r_2^{e_2-1}, \quad \ldots, \quad d_k \nmid r_k^{e_k-1}.$$

Proof. Suppose that $\mathcal{S}$ corresponds to G/f and let $g_1, g_2, \ldots, g_m$ be the unique polynomials in $\mathbb{F}_q[x]$ for which $G = \xi_1 g_1 + \xi_2 g_2 + \cdots + \xi_m g_m$. If d is the minimal polynomial of $\mathcal{S}$ then trivially d is of the form $d = d_1 d_2 \cdots d_k$, where $d_1, d_2, \ldots, d_k \in \mathbb{F}_{q^m}[x]$ and

$$d_1 \mid r_1^{e_1}, \quad d_2 \mid r_2^{e_2}, \quad \ldots, \quad d_k \mid r_k^{e_k}.$$

Suppose that without loss of generality $d_1 \mid r_1^{e_1-1}$. Then r_1 divides f/d, and consequently $G/f = G_1/d$ implies that r_1 divides $G = G_1 f/d$. With [5, Proposition 1.2] we obtain that r_1 divides $g_1, g_2, \ldots, g_m$, thus $(g_1, g_2, \ldots, g_m, f) \neq 1$ and f is not the minimal polynomial of $\boldsymbol{S} \in \mathcal{M}^{(m)}_q(f)$ for which we have $\mathcal{S} = \mathcal{S}(\boldsymbol{S}, \boldsymbol{\xi})$.

Suppose conversely that $d_i \nmid r_i^{e_i-1}$ for $i = 1, 2, \ldots, k$, but $(g_1, g_2, \ldots, g_m, f) \neq 1$. Then r_i divides g_j, $1 \leqslant j \leqslant m$, for an integer i, $1 \leqslant i \leqslant k$. Consequently by [5, Proposition 1.2] r_i divides G, and $d = f/\gcd(G, f)$ (where the greatest common divisor is calculated over $\mathbb{F}_{q^m}$) contradicts $d_i \nmid r_i^{e_i-1}$. □

Remark 2.2. Note that Proposition 2.1 implies that, amongst others, $\widehat{\mathcal{N}}^{(1)}_{q^m,\boldsymbol{\xi}}(f)$ is independent from the choice of the ordered basis $\boldsymbol{\xi}$, and we can simply write $\widehat{\mathcal{N}}^{(1)}_{q^m}(f)$ instead of $\widehat{\mathcal{N}}^{(1)}_{q^m,\boldsymbol{\xi}}(f)$. Similarly the expectation $\widehat{\mathrm{E}}_{q^m}(f)$ and the variance $\widehat{\mathrm{V}}\mathrm{ar}_{q^m}(f)$ are independent from the choice of the ordered basis $\boldsymbol{\xi}$, and hence in the following we will not include $\boldsymbol{\xi}$ in the notations $\widehat{\mathrm{E}}_{q^m}(f)$ and $\widehat{\mathrm{V}}\mathrm{ar}_{q^m}(f)$ for the expected value and the variance.

The following definitions are useful.

Definition 2.3. Let $f \in \mathbb{F}_q[x]$ be a monic polynomial with canonical factorization

$$f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$$

into irreducibles over $\mathbb{F}_q$. We define $\widehat{S}_{q^m,1}(f)$ and $\widehat{S}_{q^m,2}(f)$ as

$$\widehat{S}_{q^m,1}(f) = \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \cdots \sum_{\substack{d_k \mid r_k^{e_k} \\ d_k \nmid r_k^{e_k-1}}} \Phi^{(1)}_{q^m}(d_1 d_2 \cdots d_k) \deg(d_1 d_2 \cdots d_k),$$

and

$$\widehat{S}_{q^m,2}(f) = \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \cdots \sum_{\substack{d_k \mid r_k^{e_k} \\ d_k \nmid r_k^{e_k-1}}} \Phi^{(1)}_{q^m}(d_1 d_2 \cdots d_k) \big(\deg(d_1 d_2 \cdots d_k)\big)^2,$$

where the summations are over monic polynomials $d_i \in \mathbb{F}_{q^m}[x]$ such that $d_i \mid r_i^{e_i}$ and $d_i \nmid r_i^{e_i-1}$.

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

The identities in the following lemma will be used in Section 3.

Lemma 2.4. *Let $r_1, r_2, \ldots, r_k$ be distinct irreducible polynomials in $\mathbb{F}_q[x]$ and $e_1, e_2, \ldots, e_k$ be positive integers. We have*

$$\frac{\widehat{S}_{q^m,1}(r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k})}{\prod_{i=1}^{k}(q^{me_i \deg(r_i)} - q^{m(e_i-1)\deg(r_i)})} = \sum_{i=1}^{k} \frac{\widehat{S}_{q^m,1}(r_i^{e_i})}{q^{me_i \deg(r_i)} - q^{m(e_i-1)\deg(r_i)}}, \tag{2.3}$$

and

$$\begin{aligned}
&\frac{\widehat{S}_{q^m,2}(r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k})}{\prod_{i=1}^{k}(q^{me_i \deg(r_i)} - q^{m(e_i-1)\deg(r_i)})} \\
&\quad = \sum_{i=1}^{k} \frac{\widehat{S}_{q^m,2}(r_i^{e_i})}{q^{me_i \deg(r_i)} - q^{m(e_i-1)\deg(r_i)}} \\
&\qquad + 2 \sum_{1 \leqslant i < j \leqslant k} \frac{\widehat{S}_{q^m,1}(r_i^{e_i})}{q^{me_i \deg(r_i)} - q^{m(e_i-1)\deg(r_i)}} \frac{\widehat{S}_{q^m,1}(r_j^{e_j})}{q^{me_j \deg(r_j)} - q^{m(e_j-1)\deg(r_j)}}.
\end{aligned} \tag{2.4}$$

Proof. The identities are trivial if $k = 1$. Assume that $k = 2$. With (2.2) we have

$$\widehat{S}_{q^m,1}\big(r_1^{e_1} r_2^{e_2}\big) = \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \Phi_{q^m}^{(1)}(d_1) \Phi_{q^m}^{(1)}(d_2) \big(\deg(d_1) + \deg(d_2)\big).$$

Then we get

$$\begin{aligned}
\widehat{S}_{q^m,1}\big(r_1^{e_1} r_2^{e_2}\big) &= \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \Phi_{q^m}^{(1)}(d_1) \deg(d_1) \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \Phi_{q^m}^{(1)}(d_2) \\
&\quad + \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \Phi_{q^m}^{(1)}(d_2) \deg(d_2) \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \Phi_{q^m}^{(1)}(d_1) \\
&= \widehat{S}_{q^m,1}\big(r_1^{e_1}\big)\big(q^{me_2 \deg(r_2)} - q^{m(e_2-1)\deg(r_2)}\big) \\
&\quad + \widehat{S}_{q^m,1}\big(r_2^{e_2}\big)\big(q^{me_1 \deg(r_1)} - q^{m(e_1-1)\deg(r_1)}\big),
\end{aligned} \tag{2.5}$$

where the identity

$$\sum_{\substack{d_i \mid r_i^{e_i} \\ d_i \nmid r_i^{e_i-1}}} \Phi_{q^m}^{(1)}(d_i) = \big(q^{me_i \deg(r_i)} - q^{m(e_i-1)\deg(r_i)}\big) \tag{2.6}$$

for $i = 1, 2$ follows from (2.1). Dividing both sides of (2.5) by $\prod_{i=1}^{2}(q^{me_i \deg(r_i)} - q^{m(e_i-1)\deg(r_i)})$ we obtain (2.3) for $k = 2$. We complete the proof of (2.3) by induction on k using similar arguments. Again for $k = 2$, we have

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

$$\widehat{S}_{q^m,2}\big(r_1^{e_1}r_2^{e_2}\big) = \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \Phi_{q^m}^{(1)}(d_1)\Phi_{q^m}^{(1)}(d_2) \times \big(\big(\deg(d_1)\big)^2 + \big(\deg(d_2)\big)^2 + 2\deg(d_1)\deg(d_2)\big).$$

Then we get

$$\begin{aligned}\widehat{S}_{q^m,2}\big(r_1^{e_1}r_2^{e_2}\big) = {} & \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \Phi_{q^m}^{(1)}(d_1)\big(\deg(d_1)\big)^2 \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \Phi_{q^m}^{(1)}(d_2) \\ & + \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \Phi_{q^m}^{(1)}(d_2)\big(\deg(d_2)\big)^2 \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \Phi_{q^m}^{(1)}(d_1) \\ & + 2 \sum_{\substack{d_1 \mid r_1^{e_1} \\ d_1 \nmid r_1^{e_1-1}}} \Phi_{q^m}^{(1)}(d_1)\deg(d_1) \sum_{\substack{d_2 \mid r_2^{e_2} \\ d_2 \nmid r_2^{e_2-1}}} \Phi_{q^m}^{(1)}(d_2)\deg(d_2),\end{aligned}$$

and hence

$$\begin{aligned}\widehat{S}_{q^m,2}\big(r_1^{e_1}r_2^{e_2}\big) = {} & \widehat{S}_{q^m,2}\big(r_1^{e_1}\big)\big(q^{me_2\deg(r_2)} - q^{m(e_2-1)\deg(r_2)}\big) \\ & + \widehat{S}_{q^m,2}\big(r_2^{e_2}\big)\big(q^{me_1\deg(r_1)} - q^{m(e_1-1)\deg(r_1)}\big) + 2\widehat{S}_{q^m,1}\big(r_1^{e_1}\big)\widehat{S}_{q^m,1}\big(r_2^{e_2}\big). \qquad (2.7)\end{aligned}$$

Dividing both sides of (2.7) by $\prod_{i=1}^{2}(q^{me_i\deg(r_i)} - q^{m(e_i-1)\deg(r_i)})$ we obtain (2.4) for $k = 2$. We complete the proof of (2.4) by induction on k using similar arguments. □

3. Main results

In [2, Theorem 3.4] exact formulas for the expected value $\mathrm{E}^{(m)}(f)$ and the variance $\mathrm{Var}^{(m)}(f)$ of the joint linear complexity of a random m-fold multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ has been presented: Let $f = r_1^{e_1}r_2^{e_2}\cdots r_k^{e_k}$ be the canonical factorization of f into monic irreducible polynomials over $\mathbb{F}_q$, then

$$\mathrm{E}^{(m)}(f) = \deg(f) - \sum_{i=1}^{k} \frac{1-\alpha_i^{-e_i}}{\alpha_i - 1}\deg(r_i), \qquad (3.1)$$

$$\mathrm{Var}^{(m)}(f) = \sum_{i=1}^{k}\left(\frac{\deg(r_i)}{1-\alpha_i^{-1}}\right)^2\big((2e_i+1)\big(\alpha_i^{-e_i-2} - \alpha_i^{-e_i-1}\big) - \alpha_i^{-2e_i-2} + \alpha_i^{-1}\big),$$

where $\alpha_i = q^{m\deg(r_i)}$ for $1 \leqslant i \leqslant k$. In this section we present the expected value $\widehat{\mathrm{E}}_{q^m}(f)$ and the variance $\widehat{\mathrm{V}}\mathrm{ar}_{q^m}(f)$ for the generalized joint linear complexity of a random m-fold multisequence $\boldsymbol{S} \in \mathcal{M}_q^{(m)}(f)$ with the maximal possible joint linear complexity $\deg(f)$. The result on the expected value generalizes the result on N-periodic multisequences given in [4, Theorem 3].

Theorem 3.1. *Let $r_1, r_2, \ldots, r_k$ be distinct irreducible polynomials in $\mathbb{F}_q[x]$ and $e_1, e_2, \ldots, e_k$ be positive integers. We have*

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

$$\widehat{\mathrm{E}}_{q^m}\left(r_1^{e_1}r_2^{e_2}\cdots r_k^{e_k}\right)=\sum_{i=1}^{k}\widehat{\mathrm{E}}_{q^m}\left(r_i^{e_i}\right),$$

and

$$\widehat{\mathrm{V}}\mathrm{ar}_{q^m}\left(r_1^{e_1}r_2^{e_2}\cdots r_k^{e_k}\right)=\sum_{i=1}^{k}\widehat{\mathrm{V}}\mathrm{ar}_{q^m}\left(r_i^{e_i}\right).$$

Proof. With Definition 2.3, (2.6) and (2.3) we obtain

$$\sum_{i=1}^{k}\widehat{\mathrm{E}}_{q^m}\left(r_i^{e_i}\right)=\sum_{i=1}^{k}\frac{\widehat{S}_{q^m,1}(r_i^{e_i})}{q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}}=\frac{\widehat{S}_{q^m,1}(r_1^{e_1}r_2^{e_2}\cdots r_k^{e_k})}{\prod_{i=1}^{k}(q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)})}. \tag{3.2}$$

Hence it remains to show that

$$\prod_{i=1}^{k}\left(q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}\right)=\sum_{\substack{d_1\mid r_1^{e_1}\\ d_1\nmid r_1^{e_1-1}}}\sum_{\substack{d_2\mid r_2^{e_2}\\ d_2\nmid r_2^{e_2-1}}}\cdots\sum_{\substack{d_k\mid r_k^{e_k}\\ d_k\nmid r_k^{e_k-1}}}\Phi_{q^m}^{(1)}(d_1d_2\cdots d_k). \tag{3.3}$$

For $k=2$ with (2.6) and (2.2) we obtain

$$\prod_{i=1}^{2}\left(q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}\right)=\prod_{i=1}^{2}\sum_{\substack{d_i\mid r_i^{e_i}\\ d_i\nmid r_i^{e_i-1}}}\Phi_{q^m}^{(1)}(d_i)=\sum_{\substack{d_1\mid r_1^{e_1}\\ d_1\nmid r_1^{e_1-1}}}\sum_{\substack{d_2\mid r_2^{e_2}\\ d_2\nmid r_2^{e_2-1}}}\Phi_{q^m}^{(1)}(d_1d_2).$$

We complete the proof on the expectation by induction on k. Next we consider the variance. With Definition 2.3, (2.4), (3.2) and (3.3) we obtain

$$\begin{aligned}\widehat{\mathrm{V}}\mathrm{ar}_{q^m}\left(r_1^{e_1}r_2^{e_2}\cdots r_k^{e_k}\right)&=\frac{\widehat{S}_{q^m,2}(f)}{\Phi_q^{(m)}(f)}-\left(\frac{\widehat{S}_{q^m,1}(f)}{\Phi_q^{(m)}(f)}\right)^2\\&=\sum_{i=1}^{k}\frac{\widehat{S}_{q^m,2}(r_i^{e_i})}{q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}}\\&\quad+2\sum_{1\leqslant i<j\leqslant k}\frac{\widehat{S}_{q^m,1}(r_i^{e_i})}{q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}}\frac{\widehat{S}_{q^m,1}(r_j^{e_j})}{q^{me_j\deg(r_j)}-q^{m(e_j-1)\deg(r_j)}}\\&\quad-\left(\sum_{i=1}^{k}\frac{\widehat{S}_{q^m,1}(r_i^{e_i})}{q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}}\right)^2\\&=\sum_{i=1}^{k}\left(\frac{\widehat{S}_{q^m,2}(r_i^{e_i})}{q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}}-\left(\frac{\widehat{S}_{q^m,1}(r_i^{e_i})}{q^{me_i\deg(r_i)}-q^{m(e_i-1)\deg(r_i)}}\right)^2\right)\\&=\sum_{i=1}^{k}\widehat{\mathrm{V}}\mathrm{ar}_{q^m}\left(r_i^{e_i}\right).\qquad\square\end{aligned}$$

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

Before we present formulas for $\widehat{\mathrm{E}}_{q^m}(f)$ and $\widehat{\mathrm{V}}\mathrm{ar}_{q^m}(f)$ if $f = r^e$, $r \in \mathbb{F}_q[x]$ irreducible, we recall some definitions and identities from [2]: For a monic polynomial $f \in \mathbb{F}_q[x]$, let

$$S_{q,1}(f) = \sum_{d|f} \Phi_q^{(1)}(d)\deg(d), \tag{3.4}$$

and

$$S_{q,2}(f) = \sum_{d|f} \Phi_q^{(1)}(d)\big(\deg(d)\big)^2,$$

where the summation is over monic polynomials $d \in \mathbb{F}_q[x]$ dividing f. If $f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$ is the canonical factorization of f into monic irreducible polynomials over $\mathbb{F}_q$ and $\alpha_i = q^{\deg(r_i)}$, then (see [2, Proposition 3.2])

$$S_{q,1}(f) = q^{\deg(f)} \sum_{i=1}^{k} \frac{S_{q,1}(r_i^{e_i})}{\alpha_i^{e_i}}, \tag{3.5}$$

$$S_{q,2}(f) = q^{\deg(f)} \left(\sum_{i=1}^{k} \frac{S_{q,2}(r_i^{e_i})}{\alpha_i^{e_i}} + 2 \sum_{1 \leqslant i < j \leqslant k} \frac{S_{q,1}(r_i^{e_i})}{\alpha_i^{e_i}} \frac{S_{q,1}(r_j^{e_j})}{\alpha_j^{e_j}} \right). \tag{3.6}$$

Particularly, if $f = r^e$ with $r \in \mathbb{F}_q[x]$ irreducible, then (see [2, Eqs. (3.9) and (3.12)])

$$\frac{S_{q,1}(r^e)}{\alpha^e} = \deg(r)\left(e - \frac{1-\alpha^{-e}}{\alpha - 1}\right), \tag{3.7}$$

$$\frac{S_{q,2}(r^e)}{\alpha^e} = \left(\frac{\deg(r)}{\alpha - 1}\right)^2 \big(e^2\alpha^2 - \big(2e^2 + 2e - 1\big)\alpha + (e+1)^2 - \alpha^{1-e} - \alpha^{-e}\big), \tag{3.8}$$

where $\alpha = q^{\deg(r)}$.

Proposition 3.2. *Let r be an irreducible polynomial in $\mathbb{F}_q[x]$, and e, m be positive integers, and suppose that $u = \gcd(\deg(r), m)$. Then with $\beta = q^{\frac{m}{u}\deg(r)}$ we have*

$$\widehat{\mathrm{E}}_{q^m}\big(r^e\big) = e\deg(r) - \deg(r)\left(\frac{1-\beta^{-e}}{\beta - 1} - \frac{1-\beta^{-e}}{\beta^u - 1}\right), \tag{3.9}$$

and

$$\begin{aligned}\widehat{\mathrm{V}}\mathrm{ar}_{q^m}\big(r^e\big) = \frac{1}{u}\left(\frac{\deg(r)}{(\beta-1)(1-\beta^{-u})}\right)^2 &\big(\beta - (2e+1)\beta^{1-e} + (2e+1)\beta^{-e} - \beta^{-2e} \\ &+ \beta^{-u}\big(\big(\beta^{-e}-1\big)\big[2\beta + \beta^{-e} + \beta^{2-e} - u(\beta-1)^2\big(\beta^{-e}-1\big)\big] + 2e\beta^{-e}\big(\beta^2-1\big)\big) \\ &+ \beta^{-2u}\big(\beta - (2e-1)\beta^{2-e} + (2e-1)\beta^{1-e} - \beta^{2-2e}\big)\big).\end{aligned} \tag{3.10}$$

Proof. Note that

$$\widehat{\mathrm{E}}_{q^m}\big(r^e\big) = \frac{\widehat{S}_{q^m,1}(r^e)}{q^{me\deg(r)} - q^{m(e-1)\deg(r)}} \tag{3.11}$$

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

and

$$\widehat{S}_{q^m,1}(r^e) = S_{q^m,1}(r^e) - S_{q^m,1}(r^{e-1}). \tag{3.12}$$

By [6, Theorem 3.46] the canonical factorization of r into irreducibles over $\mathbb{F}_{q^m}$ is of the form

$$r = \rho_1 \rho_2 \cdots \rho_u, \tag{3.13}$$

where $\deg(\rho_i) = \deg(r)/u$. With (3.5) we have

$$S_{q^m,1}(r^e) = q^{me\deg(r)} \sum_{i=1}^{u} \frac{S_{q^m,1}(\rho_i^e)}{\beta^e}. \tag{3.14}$$

For $1 \leqslant i \leqslant u$, from $\mathrm{E}^{(1)}(\rho_i^e) = S_{q^m,1}(\rho_i^e)/\beta^e$ and (3.1) we get

$$\frac{S_{q^m,1}(\rho_i^e)}{\beta^e} = \frac{\deg(r)}{u}\left(e - \frac{1-\beta^{-e}}{\beta-1}\right). \tag{3.15}$$

Using (3.14) and (3.15) we obtain that

$$S_{q^m,1}(r^e) = q^{me\deg(r)} \deg(r)\left(e - \frac{1-\beta^{-e}}{\beta-1}\right), \tag{3.16}$$

and similarly

$$S_{q^m,1}(r^{e-1}) = q^{m(e-1)\deg(r)} \deg(r)\left(e - 1 - \frac{1-\beta^{-e+1}}{\beta-1}\right). \tag{3.17}$$

Note that

$$e - 1 - \frac{1-\beta^{-e+1}}{\beta-1} = \left(e - \frac{1-\beta^{-e}}{\beta-1}\right) - \left(1-\beta^{-e}\right). \tag{3.18}$$

Combining (3.16)–(3.18) we get

$$\frac{S_{q^m,1}(r^e) - S_{q^m,1}(r^{e-1})}{q^{me\deg(r)} - q^{m(e-1)\deg(r)}} = e\deg(r) - \deg(r)\frac{1-\beta^{-e}}{\beta-1} + \deg(r)\frac{1-\beta^{-e}}{\beta^u-1}. \tag{3.19}$$

We complete the proof of (3.9) using (3.11), (3.12) and (3.19).

Next we consider the variance $\widehat{\mathrm{V}}\mathrm{ar}_{q^m}(r^e)$. Note that

$$\widehat{\mathrm{V}}\mathrm{ar}_{q^m}(r^e) = \frac{\widehat{S}_{q^m,2}(r^e)}{\beta^{ue}(1-\beta^{-u})} - \left(\frac{\widehat{S}_{q^m,1}(r^e)}{\beta^{ue}(1-\beta^{-u})}\right)^2 \tag{3.20}$$

and as in (3.12) we have

$$\widehat{S}_{q^m,2}(r^e) = S_{q^m,2}(r^e) - S_{q^m,2}(r^{e-1}). \tag{3.21}$$

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

We consider $A(e,\beta)$ and $B(e,\beta)$ as functions on the integer variables e and β given by

$$A(e,\beta) = e^2\beta^2 - \big(2e^2+2e-1\big)\beta + (e+1)^2 - \beta^{1-e} - \beta^{-e}, \quad \text{and}$$
$$B(e,\beta) = e\beta - (e+1) + \beta^{-e}. \tag{3.22}$$

Recall that the canonical factorization of $r \in \mathbb{F}_q[x]$ into irreducibles over $\mathbb{F}_{q^m}$ is given in (3.13). For each $1 \leqslant i \leqslant u$, using Eqs. (3.8) and (3.7), we obtain

$$\frac{S_{q^m,2}(\rho_i^e)}{\beta^e} = \left(\frac{\deg(r)}{u(\beta-1)}\right)^2 A(e,\beta),$$

and

$$\frac{S_{q^m,1}(\rho_i^e)}{\beta^e} = \frac{\deg(r)}{u(\beta-1)} B(e,\beta),$$

respectively. By (3.6) we have

$$S_{q^m,2}\big(r^e\big) = \beta^{ue}\left(\sum_{i=1}^{u} \frac{S_{q^m,2}(\rho_i^e)}{\beta^e} + 2\sum_{1\leqslant i<j\leqslant u} \frac{S_{q^m,1}(\rho_i^e)}{\beta^e}\frac{S_{q^m,1}(\rho_j^e)}{\beta^e}\right),$$

and hence using (3.21) we get

$$\frac{\widehat{S}_{q^m,2}(r^e)}{\beta^{ue}(1-\beta^{-u})} = \left(\frac{\deg(r)}{u(\beta-1)}\right)^2 \frac{1}{1-\beta^{-u}}\big(uA(e,\beta) + \big(u^2-u\big)B(e,\beta)^2 - \beta^{-u}\big(uA(e-1,\beta) + \big(u^2-u\big)B(e-1,\beta)^2\big)\big). \tag{3.23}$$

Similarly

$$\frac{\widehat{S}_{q^m,1}(r^e)}{\beta^{ue}(1-\beta^{-u})} = \frac{\deg(r)}{u(\beta-1)}\frac{1}{1-\beta^{-u}}\big(uB(e,\beta) - u\beta^{-u}B(e-1,\beta)\big). \tag{3.24}$$

We complete the proof of (3.10) using (3.20), (3.22)–(3.24). □

Combining Theorem 3.1 and Proposition 3.2 we obtain the following result.

Theorem 3.3. *Let $f \in \mathbb{F}_q[x]$ be a monic polynomial with $\deg(f) \geqslant 1$ and canonical factorization*

$$f = r_1^{e_1} r_2^{e_2} \cdots r_k^{e_k}$$

into irreducibles over $\mathbb{F}_q$. For $1 \leqslant i \leqslant k$ let $u_i = \gcd(\deg(r_i), m)$ and

$$\beta_i = q^{\frac{m}{u_i}\deg(r_i)}.$$

Then we have

$$\widehat{\mathrm{E}}_{q^m}(f) = \deg(f) - \sum_{i=1}^{k} \deg(r_i)\left(\frac{1-\beta_i^{-e_i}}{\beta_i - 1} - \frac{1-\beta_i^{-e_i}}{\beta_i^{u_i}-1}\right),$$

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

and

$$\widehat{\mathrm{V}}\mathrm{ar}_{q^m}(f)=\sum_{i=1}^{k}\Bigg\{\frac{1}{u_i}\bigg(\frac{\deg(r_i)}{(\beta_i-1)(1-\beta_i^{-u_i})}\bigg)^2\big(\beta_i-(2e_i+1)\beta_i^{1-e_i}+(2e_i+1)\beta_i^{-e_i}-\beta_i^{-2e_i}$$
$$+\beta_i^{-u_i}\big((\beta_i^{-e_i}-1)\big[2\beta_i+\beta_i^{-e_i}+\beta_i^{2-e_i}-u_i(\beta_i-1)^2(\beta_i^{-e_i}-1)\big]+2e_i\beta_i^{-e_i}(\beta_i^2-1)\big)$$
$$+\beta_i^{-2u_i}\big(\beta_i-(2e_i-1)\beta_i^{2-e_i}+(2e_i-1)\beta_i^{1-e_i}-\beta_i^{2-2e_i}\big)\big)\Bigg\}.$$

In the following we want to estimate the expected drop of the linear complexity if one switches from conventional joint linear complexity to generalized joint linear complexity. We consider the term

$$D(\boldsymbol{S}):=\frac{L_q^{(m)}(\boldsymbol{S})-L_{q^m,\xi}(\boldsymbol{S})}{L_q^{(m)}(\boldsymbol{S})},$$

the difference of joint linear complexity and generalized joint linear complexity in relation to the value for the joint linear complexity, where we put $D(\mathbf{0})=0$ by convention if $\boldsymbol{S}$ is the zero sequence $\mathbf{0}$ (or, equivalently, if $L_q^{(m)}(\boldsymbol{S})=0$). In [5, Corollary 1] it has been shown that $D(\boldsymbol{S})\leqslant 1-\frac{1}{u_{\max}}$ if $\boldsymbol{S}\in\mathcal{M}_q^{(m)}(f)$, $f=r_1^{e_1}r_2^{e_2}\cdots r_k^{e_k}$ and $u_{\max}=\max\{\gcd(\deg(r_i),m)\colon\ 1\leqslant i\leqslant k\}$. We are now interested in the expected value of $D(\boldsymbol{S})$ for a random multisequence $\boldsymbol{S}\in\mathcal{M}_q^{(m)}(f)$. The results confirm that though the bound on $D(\boldsymbol{S})$ has been shown to be tight (see [5, Proposition 3]), in average linear complexity does not decrease dramatically if one switches from conventional joint linear complexity to generalized joint linear complexity.

Proposition 3.4. *Let $f\in\mathbb{F}_q[x]$ be a monic polynomial with $\deg(f)\geqslant 1$, then the expected value $\mathrm{E}_{\mathrm{drop},q}^{(m)}(f)$ of $D(\boldsymbol{S})$ for a random multisequence $\boldsymbol{S}\in\mathcal{M}_q^{(m)}(f)$ is given by*

$$\mathrm{E}_{\mathrm{drop},q}^{(m)}(f)=\frac{1}{q^{m\deg(f)}}\sum_{d|f,\,d\neq 1}\Phi_q^{(m)}(d)\bigg(1-\frac{\widehat{\mathrm{E}}_{q^m}(d)}{\deg(d)}\bigg),$$

where the summation is over all monic polynomials $d\in\mathbb{F}_q[x]$ dividing f, except $d=1$.

Proof. From the definition of $\mathrm{E}_{\mathrm{drop},q}^{(m)}(f)$ we get

$$\mathrm{E}_{\mathrm{drop},q}^{(m)}(f)=\frac{1}{|\mathcal{M}_q^{(m)}(f)|}\sum_{\boldsymbol{S}\in\mathcal{M}_q^{(m)}(f)\setminus\{\mathbf{0}\}}\frac{L_q^{(m)}(\boldsymbol{S})-L_{q^m,\xi}(\boldsymbol{S})}{L_q^{(m)}(\boldsymbol{S})}$$
$$=\frac{1}{q^{m\deg(f)}}\sum_{\boldsymbol{S}\in\mathcal{M}_q^{(m)}(f)\setminus\{\mathbf{0}\}}\bigg(1-\frac{L_{q^m,\xi}(\boldsymbol{S})}{L_q^{(m)}(\boldsymbol{S})}\bigg).\tag{3.25}$$

Recall that

$$\mathcal{M}_q^{(m)}(f)=\bigcup_{d|f}\mathcal{N}_q^{(m)}(d),\tag{3.26}$$

is the disjoint union over all monic polynomials $d\in\mathbb{F}_q[x]$ dividing f. Furthermore for a monic polynomial $d\in\mathbb{F}_q[x]$ dividing f we have

$$\left|\mathcal{N}_q^{(m)}(d)\right| = \Phi_q^{(m)}(d) \quad \text{and}$$
$$\widehat{\mathrm{E}}_{q^m}(d) = \sum_{\boldsymbol{S}\in\mathcal{N}_q^{(m)}(d)} \frac{L_{q^m,\xi}(\boldsymbol{S})}{|\mathcal{N}_q^{(m)}(d)|}. \tag{3.27}$$

Moreover if $\boldsymbol{S} \in \mathcal{N}_q^{(m)}(d)$, then by definition

$$L_q^{(m)}(\boldsymbol{S}) = \deg(d). \tag{3.28}$$

Combining (3.25)–(3.28) we complete the proof. □

We recall that for a monic polynomial $d \in \mathbb{F}_q[x]$, we have (see [2, Lemma 2.2])

$$\Phi_q^{(m)}(d) = q^{m\deg(d)} \prod_{i=1}^{l} \left(1 - q^{-m\deg(r_i)}\right), \tag{3.29}$$

if $d = r_1^{a_1} r_2^{a_2} \cdots r_l^{a_l}$ is the canonical factorization of d over $\mathbb{F}_q$. Moreover $\widehat{\mathrm{E}}_{q^m}(d)$ is given by Theorem 3.3. Therefore Proposition 3.4 gives a procedure to determine $\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(f)$ in the general case. In the following corollaries we present closed formulas on the expected drop of the linear complexity for two special cases.

Corollary 3.5. *Let r be an irreducible polynomial in $\mathbb{F}_q[x]$, let e, m be positive integers and suppose that $u = \gcd(\deg(r), m)$. Then $\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(r^e)$ is given by*

$$\mathrm{E}^{(m)}_{\mathrm{drop},\,q}\left(r^e\right) = \frac{\beta^{u-1}-1}{\beta^{u(e+1)-1}(\beta-1)}\left(H_e\left(\beta^u\right) - H_e\left(\beta^{u-1}\right)\right),$$

where $\beta = q^{\frac{m}{u}\deg(r)}$ and $H_e(x)$ is the real valued function defined by

$$H_e(x) = x + \frac{x^2}{2} + \cdots + \frac{x^e}{e}.$$

Proof. From Eq. (3.29) we obtain

$$\Phi_q^{(m)}\left(r^j\right) = q^{mj\deg(r)} - q^{m(j-1)\deg(r)} = \beta^{uj} - \beta^{u(j-1)}, \quad 1 \leqslant j \leqslant e,$$

and consequently with Proposition 3.4

$$\mathrm{E}^{(m)}_{\mathrm{drop},\,q}\left(r^e\right) = \frac{1}{q^{me\deg(r)}} \sum_{j=1}^{e} \left(\beta^{uj} - \beta^{u(j-1)}\right)\left(1 - \frac{\widehat{\mathrm{E}}_{q^m}(r^j)}{j\deg(r)}\right).$$

Using Theorem 3.3 we get

$$\begin{aligned}\mathrm{E}^{(m)}_{\mathrm{drop},\,q}\left(r^e\right) &= \frac{1}{q^{me\deg(r)}} \sum_{j=1}^{e} \left(\beta^{uj} - \beta^{u(j-1)}\right)\left(1 - \frac{j\deg(r) - \deg(r)\left(\frac{1-\beta^{-j}}{\beta-1} - \frac{1-\beta^{-j}}{\beta^u-1}\right)}{j\deg(r)}\right)\\ &= \frac{1}{q^{me\deg(r)}} \sum_{j=1}^{e} \frac{1}{j}\left(\frac{1-\beta^{-j}}{\beta-1} - \frac{1-\beta^{-j}}{\beta^u-1}\right)\beta^{uj}\left(1-\beta^{-u}\right).\end{aligned}$$

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

With

$$\left(\frac{1-\beta^{-j}}{\beta-1}-\frac{1-\beta^{-j}}{\beta^u-1}\right)(1-\beta^{-u})=\frac{(1-\beta^{-j})(\beta^{u-1}-1)}{\beta^{u-1}(\beta-1)}$$

we obtain

$$\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(r^e)=\frac{1}{q^{me\deg(r)}}\sum_{j=1}^{e}\frac{1}{j}\beta^{uj}\frac{(1-\beta^{-j})(\beta^{u-1}-1)}{\beta^{u-1}(\beta-1)}$$

and the claim of the corollary follows. □

Corollary 3.6. *Let $r_1,\ldots,r_k\in\mathbb{F}_q[x]$ be distinct irreducible polynomials such that $\deg(r_i)=l$ for each $1\leqslant i\leqslant k$. Let $f=r_1\cdots r_k\in\mathbb{F}_q[x]$, m be a positive integer, and $u=\gcd(l,m)$. Then $\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(f)$ is given by*

$$\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(f)=\frac{q^{m\deg(f)}-1}{q^{m\deg(f)}}\left(\frac{1-\beta^{-1}}{\beta-1}-\frac{1-\beta^{-1}}{\beta^u-1}\right),$$

where $\beta=q^{\frac{m}{u}\deg(r)}$.

Proof. Assume that $\rho_1,\ldots,\rho_t\in\mathbb{F}_q[x]$ are distinct irreducible polynomials of degree l and put $d=\rho_1\cdots\rho_t\in\mathbb{F}_q[x]$. Then with Theorem 3.3 we obtain

$$\widehat{\mathrm{E}}_{q^m}(d)=lt-\sum_{i=1}^{t}l\left(\frac{1-\beta^{-1}}{\beta-1}-\frac{1-\beta^{-1}}{\beta^u-1}\right),\tag{3.30}$$

where $\beta=q^{\frac{m}{u}\deg(r)}$. From Eq. (3.29) we obtain

$$\Phi^{(m)}_q(d)=\left(q^{ml}-1\right)^t,$$

and thus

$$\begin{aligned}\Phi^{(m)}_q(d)\left(1-\frac{\widehat{\mathrm{E}}_{q^m}(d)}{\deg(d)}\right)&=\left(q^{ml}-1\right)^t\left(1-\frac{lt-\sum_{i=1}^{t}l(\frac{1-\beta^{-1}}{\beta-1}-\frac{1-\beta^{-1}}{\beta^u-1})}{lt}\right)\\&=\left(q^{ml}-1\right)^t\frac{1}{t}\sum_{i=1}^{t}\left(\frac{1-\beta^{-1}}{\beta-1}-\frac{1-\beta^{-1}}{\beta^u-1}\right)\\&=\left(q^{ml}-1\right)^t\left(\frac{1-\beta^{-1}}{\beta-1}-\frac{1-\beta^{-1}}{\beta^u-1}\right).\end{aligned}$$

Consequently, for f as defined in the corollary, using Proposition 3.4 we obtain that

$$\begin{aligned}q^{m\deg(f)}\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(f)&=\sum_{t=1}^{k}\binom{k}{t}\left(q^{ml}-1\right)^t\left(\frac{1-\beta^{-1}}{\beta-1}-\frac{1-\beta^{-1}}{\beta^u-1}\right)\\&=\left(q^{mlk}-1\right)\left(\frac{1-\beta^{-1}}{\beta-1}-\frac{1-\beta^{-1}}{\beta^u-1}\right).\end{aligned}$$

□

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

Remark 3.7. Let N be a prime and l be the order of q modulo N, then the canonical factorization of $x^N-1 \in \mathbb{F}_q[x]$ is given by

$$x^N-1=(x-1)r_1r_2\cdots r_{(N-1)/l},$$

where $r_1, r_2, \ldots, r_{(N-1)/l}$ are distinct irreducible polynomials of degree l. Let S be an N-periodic sequence, then $S \in \mathcal{M}_q^{(1)}(f)$ with $f=r_1r_2\cdots r_{(N-1)/l}$ if and only if S has the *zero sum property*, i.e. the elements of one period of S sum up to zero. Conversely every sequence in $S \in \mathcal{M}_q^{(1)}(f)$, $f=r_1r_2\cdots r_{(N-1)/l}$, is N-periodic. Consequently Corollary 3.6 also gives the expected value for $D(\boldsymbol{S})$ for a random N-periodic m-fold multisequence with zero sum property in each component.

Remark 3.8. At a first glance one might think that $\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(f)$ is equal to

$$\frac{\mathrm{E}_q^{(m)}(f)-\mathrm{E}_{q^m}^{(1)}(f)}{\mathrm{E}_q^{(m)}(f)}.$$

However they are different. For example let $q=2$. Using Corollary 3.5 for $f=(x^2+x+1)^2$ we obtain that

$$\mathrm{E}^{(2)}_{\mathrm{drop},\,2}(f)=\tfrac{33}{256}=0.1289062\ldots, \quad \text{and}$$

$$\frac{\mathrm{E}_2^{(2)}(f)-\mathrm{E}_{2^2}^{(1)}(f)}{\mathrm{E}_2^{(2)}(f)}=\tfrac{7}{55}=0.1272727\ldots.$$

Similarly, using Corollary 3.6 for $f=(x^3+x+1)(x^3+x^2+1)$ we obtain that

$$\mathrm{E}^{(3)}_{\mathrm{drop},\,2}(f)=\frac{32319}{262144}=0.1232872\ldots, \quad \text{and}$$

$$\frac{\mathrm{E}_2^{(3)}(f)-\mathrm{E}_{2^3}^{(1)}(f)}{\mathrm{E}_2^{(3)}(f)}=\frac{9}{73}=0.1232876\ldots.$$

In the following example we illustrate how to use Proposition 3.4 as a procedure to determine $\mathrm{E}^{(m)}_{\mathrm{drop},\,q}(f)$.

Example 3.9. Let $q=2$, $m=6$ and $f=(x^2+x+1)^2(x^3+x+1)$. Note that the closed formulas in Corollaries 3.5 and 3.6 do not apply for the computation of $\mathrm{E}^{(6)}_{\mathrm{drop},\,2}(f)$ in this case. Let $d_1=x^2+x+1$, $d_2=(x^2+x+1)^2$, $d_3=x^3+x+1$, $d_4=(x^2+x+1)(x^3+x+1)$, and $d_5=(x^2+x+1)^2(x^3+x+1)$. Then using (3.29) we obtain that

$$\begin{aligned}
&\Phi_2^{(6)}(d_1)=4095,\\
&\Phi_2^{(6)}(d_2)=16773120,\\
&\Phi_2^{(6)}(d_3)=262143,\\
&\Phi_2^{(6)}(d_4)=1073475585,\\
&\Phi_2^{(6)}(d_5)=4396955996160.
\end{aligned} \tag{3.31}$$

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004

Moreover from Theorem 3.3 we get

$$\begin{aligned}
\widehat{\mathrm{E}}_{64}(d_1) &= 128/65 = 1.9692307\ldots,\\
\widehat{\mathrm{E}}_{64}(d_2) &= 127/32 = 3.96875,\\
\widehat{\mathrm{E}}_{64}(d_3) &= 4096/1387 = 2.9531362\ldots,\\
\widehat{\mathrm{E}}_{64}(d_4) &= 443776/90155 = 4.9223670\ldots,\\
\widehat{\mathrm{E}}_{64}(d_5) &= 307221/44384 = 6.9218862\ldots. \qquad (3.32)
\end{aligned}$$

Therefore using Proposition 3.4, (3.31) and (3.32) we obtain that

$$\mathrm{E}^{(6)}_{\mathrm{drop},\,2}\big((x^2+x+1)^2(x^3+x+1)\big) = 245414480283/21990232555520 = 0.0111601\ldots.$$

Acknowledgments

We would like to thank the anonymous referee for the very useful suggestions and comments. The second author was partially supported by TÜBİTAK under Grant No. TBAG-107T826.

References

[1] E. Dawson, L. Simpson, Analysis and design issues for synchronous stream ciphers, in: H. Niederreiter (Ed.), Coding Theory and Cryptology, World Scientific, Singapore, 2002, pp. 49–90.
[2] F.W. Fu, H. Niederreiter, F. Özbudak, Joint linear complexity of multisequences consisting of linear recurring sequences, in: Cryptography and Communications—Discrete Structures, Boolean Functions and Sequences, in press, available online at doi:10.1007/s12095-007-0001-4.
[3] P. Hawkes, G.G. Rose, Exploiting multiples of the connection polynomial in word-oriented stream ciphers, in: T. Okamoto (Ed.), Advances in Cryptology – ASIACRYPT 2000, in: Lecture Notes in Comput. Sci., vol. 1976, Springer, Berlin, 2000, pp. 303–316.
[4] W. Meidl, Discrete Fourier transform, joint linear complexity and generalized joint linear complexity of multisequences, in: T. Helleseth, et al. (Eds.), Sequences and Their Applications – SETA 2004, in: Lecture Notes in Comput. Sci., vol. 3486, Springer, Berlin, 2005, pp. 101–112.
[5] W. Meidl, F. Özbudak, Generalized joint linear complexity of linear recurring sequences, in: S.W. Golomb, et al. (Eds.), Sequences and Their Applications – SETA 2008, in: Lecture Notes in Comput. Sci., vol. 5203, Springer, Berlin, 2008, pp. 266–277.
[6] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[7] H. Niederreiter, Sequences with almost perfect linear complexity profile, in: D. Chaum, W.L. Price (Eds.), Advances in Cryptology – EUROCRYPT'87, in: Lecture Notes in Comput. Sci., vol. 304, Springer, Berlin, 1988, pp. 37–51.

Please cite this article in press as: W. Meidl, F. Özbudak, Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences, Finite Fields Appl. (2008), doi:10.1016/j.ffa.2008.09.004