Linear Filtering of Nonlinear Shift-Register Sequences

Berndt M. Gammel and Rainer Göttfert

Infineon Technologies AG
Munich, Germany

Abstract. Nonlinear n-stage feedback shift-register sequences over the finite field $\mathbb{F}_q$ of period $q^n - 1$ are investigated under linear operations on sequences. We prove that all members of an easily described class of linear combinations of shifted versions of these sequences possess useful properties for cryptographic applications: large periods, large linear complexities and good distribution properties. They typically also have good maximum order complexity values as has been observed experimentally. A running key generator is introduced based on certain nonlinear feedback shift registers with modifiable linear feedforward output functions.

1 Introduction

We investigate properties of linearly filtered nonlinear shift-register sequences of span n and period $q^n - 1$. More precisely, the underlying shift register is a nonlinear n-stage feedback shift register over $\mathbb{F}_q$ which for any nonzero initial state vector produces a periodic sequence of period $q^n - 1$. Here $\mathbb{F}_q$ denotes the finite field of order q. A linear feedforward function is applied to the stages of the nonlinear feedback shift register to produce the linearly filtered sequence. We show that under easily controlled conditions on the linear filter function, the filtered sequence will have the same period and linear complexity as the original sequence whose linear complexity typically is close to the period length. We prove that the linearly filtered sequences possess good distribution properties. Furthermore, we report experimental results regarding the maximum order complexity of linearly filtered binary nonlinear shift-register sequences.

One purpose of linear filtering a nonlinear shift-register sequence is to increase the maximum order complexity of the sequence up to a value of about twice the logarithm of the period length, a value typical for random sequences (see Jansen [6]). Another objective is to enter variability into a system deploying primitive (see Definition 1) nonlinear feedback shift registers. As an illustration we discuss in Section 5 a configurable running key generator based on primitive binary shift registers endowed with modifiable linear feedforward logics.

The here discussed concept of linearly filtering nonlinear feedback shift-register sequences mirrors the complementary concept of nonlinearly filtering linear shift register sequences. The latter concept has been treated in the literature extensively. The intent there is to generate sequences of large linear com-

plexity out of maximal period linear feedback shift-register sequences. This is approached by applying certain nonlinear functions to some shifted versions of the given linear feedback shift-register sequence. We mention the work of Groth [5], Key [7], Siegenthaler, Forré and Kleiner [21], Fúster-Sabater and Caballero-Gil [3], Massey and Serconek [11], Paterson [18], Rueppel [19], and Lam and Gong [9]. Two outstanding contributions to the challenging task of creating nonlinear feedback shift registers of maximum cycle lengths are Mykkeltveit [13] and Mykkeltveit, Siu and Tong [14].

2 Preliminaries

Throughout this paper V denotes the $\mathbb{F}_q$-vector space of all inifinite sequences of elements of the finite field $\mathbb{F}_q$. The sum of two sequences $\sigma = (s_i)_{i=0}^{\infty}$ and $\tau = (t_i)_{i=0}^{\infty}$ in V is defined by $\sigma + \tau = (s_i + t_i)_{i=0}^{\infty}$. The product of a sequence $\sigma \in V$ and a scalar $c \in \mathbb{F}_q$ is defined by $c\sigma = (cs_i)_{i=0}^{\infty}$. A useful linear operator on the vector space V is the shift operator T defined by $T\sigma = (s_{i+1})_{i=0}^{\infty}$ for all $\sigma = (s_i)_{i=0}^{\infty}$ in V. If g is an arbitrary polynomial over $\mathbb{F}_q$, then $g(T)$ is again a linear operator on V.

A sequence $\sigma \in V$ is called *periodic* if there is a positive integer r such that $s_{i+r} = s_i$ for $i = 0, 1, \ldots$. The smallest positive integer r with this property is called the *period* of σ, and we write $\mathrm{per}(\sigma) = r$. Let $\sigma \in V$ be periodic and let g be a monic polynomial over $\mathbb{F}_q$. We call g a *characteristic polynomial* of σ if the linear operator $g(T)$ annihilates σ, i.e. $g(T)\sigma = \mathbf{0}$, where $\mathbf{0}$ denotes the zero sequence of V (the sequence all of whose terms are 0). For instance, $g(x) = x^r - 1$ is a characteristic polynomial of σ, if σ is periodic with period r. For any periodic sequence $\sigma \in V$,

$$J_\sigma = \{g \in \mathbb{F}_q[x] : g(T)\sigma = \mathbf{0}\}$$

is a nonzero ideal (called the *T-annihilator* of σ) in the principal ideal domain $\mathbb{F}_q[x]$. The uniquely determined monic polynomial $m_\sigma \in \mathbb{F}_q[x]$ with $J_\sigma = (m_\sigma) = m_\sigma \mathbb{F}_q[x]$ is called the *minimal polynomial* of σ. Thus the characteristic polynomials of σ are precisely the monic polynomials in $\mathbb{F}_q[x]$ that are multiples of m_σ.

The degree of m_σ is called the *linear complexity* $L(\sigma)$ of σ. The linear complexity of σ is zero if and only if σ is the zero sequence. If $L(\sigma) \geq 1$, then $L(\sigma)$ is the length of the shortest linear feedback shift register over $\mathbb{F}_q$ that can generate σ. The majority of periodic sequences in V of given period r have linear complexities close to r (see Dai and Yang [2] and Meidl and Niederreiter [12]).

Another natural approach to the minimal polynomial of a periodic sequence makes use of generating functions. Following Niederreiter [15], [17], we associate with an arbitrary sequence $\sigma = (s_i)_{i=0}^{\infty}$ of V its generating function $G_\sigma = \sum_{i=0}^{\infty} s_i x^{-i-1}$, regarded as an element of the field $\mathbb{F}_q((x^{-1}))$ of formal Laurent series over $\mathbb{F}_q$ in the indeterminate x^{-1}. The field $\mathbb{F}_q((x^{-1}))$ contains the field $\mathbb{F}_q(x)$ of rational functions as a subfield.

Lemma 1. *Let $\sigma = (s_i)_{i=0}^{\infty}$ be a sequence of elements of $\mathbb{F}_q$, and let g be a monic polynomial over $\mathbb{F}_q$ with $g(0) \neq 0$. Then σ is a periodic sequence in V with characteristic polynomial g if and only if*

$$\sum_{i=0}^{\infty} s_i x^{-i-1} = \frac{h(x)}{g(x)} \tag{1}$$

with $h \in \mathbb{F}_q[x]$ and $\deg(h) < \deg(g)$.

Proof. The assertion follows immediately by considering the coefficients in the Laurent series expansion of $g(x) \sum_{i=0}^{\infty} s_i x^{-i-1}$. See Niederreiter [15], [17], or [16, p. 218].

The polynomial g in Lemma 1 is the minimal polynomial of σ precisely if the rational function in (1) is in reduced form, i.e. $\gcd(h, g) = 1$. If this is not the case, then we can divide the numerator h and the denominator g by $\gcd(h, g)$ to produce the reduced form. It follows that $m_\sigma = g/\gcd(h, g)$.

Notice that the polynomial $h(x) = g(x) \sum_{i=0}^{\infty} s_i x^{-i-1}$ depends only on g and the first $\deg(g)$ terms of σ. Thus the above method is a way to compute the minimal polynomial of a periodic sequence from a known characteristic polynomial and a suitable number of initial terms of the sequence. The method was first described by Willett [22], supported by a rather complicated proof. The special case for the characteristic polynomial $g(x) = x^r - 1$ appeared earlier in Laksov [8].

Let g be a monic polynomial over $\mathbb{F}_q$ of positive degree n and with $g(0) \neq 0$. The sequence $\rho = (r_i)_{i=0}^{\infty}$ in V that has g as a characteristic polynomial and whose first n terms are $r_0 = \cdots = r_{n-2} = 0$ and $r_{n-1} = 1$, is called the *impulse response sequence* for g. We have $g(x) \sum_{i=0}^{\infty} r_i x^{-i-1} = (x^n + \cdots + g_1 x + g_0)(x^{-n} + r_n x^{-n-1} + \cdots) = 1$, so that the generating function of ρ satisfies

$$\sum_{i=0}^{\infty} r_i x^{-i-1} = \frac{1}{g(x)}, \tag{2}$$

which in particular shows that g is also the minimal polynomial of ρ.

Lemma 2. *Let σ be a periodic sequence in V and let the monic polynomial g with $\deg(g) = n \geq 1$ and $g(0) \neq 0$ be a characteristic polynomial of σ. Let $\rho \in V$ be the impulse response sequence for g, and let h be a polynomial over $\mathbb{F}_q$ with $\deg(h) < \deg(g)$. The rational generating function of σ is h/g if and only if $\sigma = h(T)\rho$.*

Proof. If we multiply the left-hand side of equation (2) by x^j, where $0 \leq j \leq n - 1$, we get the generating function of $T^j\rho$. If we multiply the right-hand side of (2) by x^j, we obtain the rational function $x^j/g(x)$. Hence the rational generating function of the sequence $T^j\rho$ is $x^j/g(x)$ for $0 \leq j \leq n - 1$. Consider the rational generating function of σ:

$$\frac{h(x)}{g(x)} = \frac{h_0 + h_1 x + \cdots + h_{n-1} x^{n-1}}{g(x)} = h_0 \frac{1}{g(x)} + h_1 \frac{x}{g(x)} + \cdots + h_{n-1} \frac{x^{n-1}}{g(x)}.$$

This is equivalent to $\sigma = h_0\rho + h_1 T\rho + \cdots + h_{n-1}T^{n-1}\rho = h(T)\rho$.

If $\sigma \in V$ is periodic with $\mathrm{per}(\sigma) = r \geq 2$, then the least positive integer n such that the n-tuples $\mathbf{s}_i = (s_i, s_{i+1}, \ldots, s_{i+n-1})$, $0 \leq i \leq r-1$, are all distinct is called the *span* or the *maximum order complexity* of σ. If $\sigma \in V$ is a constant sequence, then its maximum order complexity is defined to be zero.

The periodic sequences in V of span $n \geq 1$ are precisely the output sequences of nonsingular n-stage feedback shift registers over $\mathbb{F}_q$. An n-stage feedback shift register (FSR) over $\mathbb{F}_q$ is uniquely determined by its feedback function $R : \mathbb{F}_q^n \to \mathbb{F}_q$. A sequence $\sigma = (s_i)_{i=0}^{\infty}$ in V whose terms satisfy the recurrence relation

$$s_{i+n} = R(s_i, s_{i+1}, \ldots, s_{i+n-1}) \quad \text{for } i = 0, 1, \ldots$$

is called an *output sequence of the FSR* defined by R. The n-tuple $\mathbf{s}_0 = (s_0, s_1, \ldots, s_{n-1})$ is referred to as the *initial state vector* of the sequence. The FSR is called *nonsingular* if the mapping

$$M : (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n \mapsto (x_1, \ldots, x_{n-1}, R(x_0, \ldots, x_{n-1})) \in \mathbb{F}_q^n$$

is bijective. Any output sequence of a nonsingular n-stage FSR over $\mathbb{F}_q$ is periodic. The maximum possible period is $r = q^n$ as there are q^n different n-tuples of elements of $\mathbb{F}_q$.

The FSR is called a *linear feedback shift register* (LFSR) over $\mathbb{F}_q$ if the feedback function R is linear; otherwise the FSR is called a *nonlinear feedback shift register* (NLFSR) over $\mathbb{F}_q$. If R is linear, i.e.

$$R(x_0, x_1, \ldots, x_{n-1}) = a_0x_0 + a_1x_1 + \cdots + a_{n-1}x_{n-1}$$

with $a_j \in \mathbb{F}_q$ for $0 \leq j \leq n-1$, then the associated polynomial $g \in \mathbb{F}_q[x]$ given by

$$g(x) = x^n - R(1, x, \ldots, x^{n-1}) = x^n - a_{n-1}x^{n-1} - \cdots - a_1x - a_0$$

is called the *characteristic polynomial* of the LFSR. The name is justified by the fact that g is a characteristic polynomial of any possible output sequence of the LFSR.

Definition 1. An n-stage FSR over $\mathbb{F}_q$ (linear or nonlinear) is called *primitive* if for any nonzero initial state vector of $\mathbb{F}_q^n$ the corresponding output sequence has period $q^n - 1$.

It is immediate that each primitive FSR is nonsingular. Furthermore, if R is the feedback function of a primitive n-stage FSR over $\mathbb{F}_q$ and $\mathbf{0} \in \mathbb{F}_q^n$ is the zero vector, then $R(\mathbf{0}) = 0$. As a consequence, the zero sequence is an output sequence of any primitive FSR. The attribute *primitive* for the FSR's under discussion is justified for the following reason: A linear feedback shift register is primitive (in the sense of Definition 1) if and only if its characteristic polynomial is a primitive polynomial over $\mathbb{F}_q$ (see Lidl and Niederreiter [10, Chap. 8] and Golomb [4]). In the literature, the nonzero output sequences of a primitive LFSR are also called *m-sequences*, *maximal period sequences*, or *pseudo-noise sequences*.

Any two nonzero output sequences σ and τ of some primitive n-stage FSR over $\mathbb{F}_q$ are shifted versions of each other. That is, $\tau = T^d\sigma$ for some $0 \le d \le q^n - 2$. There are exactly

$$q^{-n}(q!)^{q^{n-1}}$$

primitive n-stage FSR's over $\mathbb{F}_q$ (see Van Aardenne-Ehrenfest and De Bruijn [1]) of which only $\phi(q^n-1)/n$ are linear as there are that many primitive polynomials over $\mathbb{F}_q$ of degree n. Here ϕ is Euler's function.

3 Periodicity and linear complexity

Let σ be a sequence of elements of $\mathbb{F}_q$, and let f be a nonzero polynomial over $\mathbb{F}_q$. We call the sequence $\tau = f(T)\sigma$ a *linearly filtered* sequence derived from σ. The polynomial f is referred to as the *filter polynomial*.

Lemma 3. *Let $\sigma = (s_i)_{i=0}^{\infty}$ be a periodic sequence in V with minimal polynomial $m_\sigma \in \mathbb{F}_q[x]$, and let f be a nonzero polynomial over $\mathbb{F}_q$. The sequence $\tau = f(T)\sigma$ is periodic and its minimal polynomial is given by $m_\tau = m_\sigma / \gcd(m_\sigma, f)$.*

Proof. The assertion holds if σ is the zero sequence. Otherwise, the minimal polynomial of σ has positive degree. Let $\rho \in V$ be the impulse response sequence for the polynomial m_σ and consider $h/m_\sigma \in \mathbb{F}_q(x)$, the reduced rational generating function of σ. By Lemma 2, we have $\sigma = h(T)\rho$. It follows that $\tau = f(T)[h(T)\rho] = (fh)(T)\rho$. Let u be the uniquely determined polynomial over $\mathbb{F}_q$ with $fh \equiv u \bmod m_\sigma$ and $\deg(u) < \deg(m_\sigma)$. Since $m_\sigma(T)\rho = \mathbf{0}$, it follows that $\tau = u(T)\rho$. Another application of Lemma 2 shows that u/m_σ represents the generating function of τ. By reducing u/m_σ to lowest terms, we obtain the minimal polynomial of τ as $m_\tau = m_\sigma / \gcd(m_\sigma, u)$. However, as $u \equiv fh \bmod m_\sigma$, and since the polynomials h and m_σ are relatively prime, it follows that $\gcd(m_\sigma, u) = \gcd(m_\sigma, f)$.

Lemma 4. *Let $\sigma = (s_i)_{i=0}^{\infty}$ be a nonzero output sequence of a primitive n-stage FSR over $\mathbb{F}_q$. Then the minimal polynomial $m_\sigma \in \mathbb{F}_q[x]$ of σ is the product of distinct monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n. The polynomials x and $x-1$ do not divide the minimal polynomial m_σ.*

Proof. Let $r = \mathrm{per}(\sigma)$. The n-tuples $\mathbf{s}_i = (s_i, s_{i+1}, \ldots, s_{i+n-1})$, $0 \le i \le r-1$, run exactly through all nonzero vectors of $\mathbb{F}_q^n$. Therefore, each nonzero element of $\mathbb{F}_q$ occurs exactly q^{n-1} times among the first coordinates of those n-tuples. It follows that $s_0 + s_1 + \cdots + s_{r-1} = 0$. Since σ is periodic with period r, we get

$$s_{i+r-1} + \cdots + s_{i+1} + s_i = 0 \qquad \text{for } i = 0, 1, \ldots,$$

which means that

$$c(x) = x^{r-1} + x^{r-2} \cdots + x + 1 = \frac{x^r - 1}{x - 1} \in \mathbb{F}_q[x] \tag{3}$$

is a characteristic polynomial of σ. We have $c(1) = r \cdot 1 = (q^n - 1) \cdot 1 = -1 \neq 0$. Thus the element 1 is not a root of $c(x)$, nor is 0. Consequently, the minimal polynomial $m_\sigma(x)$, which divides $c(x)$, is neither divible by $x - 1$ nor by x. Equation (3) implies that $m_\sigma(x)$ divides $x^{r+1} - x$, which, since $r + 1 = q^n$, is the product of all monic irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n.

Let g be a monic polynomial over $\mathbb{F}_q$ of positive degree n. Consider the set $S(g)$ of all periodic sequences in V that have g as a characteristic polynomial: $S(g) = \{\sigma \in V : g(T)\sigma = \mathbf{0}\}$. The set $S(g)$ is a T-invariant, n-dimensional subspace of the vector space V. It follows that for all $\sigma \in S(g)$ and for all $f \in \mathbb{F}_q[x]$, the linearly filtered sequence $\tau = f(T)\sigma$ is in $S(g)$. The vector space $S(g)$ has a particularly simple structure if the polynomial g is primitive. In this case, $S(g) = \{\mathbf{0}, \sigma, T\sigma, \ldots, T^{r-1}\sigma\}$, where σ is an arbitrary sequence of $S(g)$ with a nonzero initial state vector and $r = q^n - 1$. It follows that the linearly filtered output sequence of a primitive LFSR is always a shifted version of the original output sequence. As linearly filtering primitive LFSR-output sequences does not produce "new" sequences we exclude the LFSR case from the following investigations.

Theorem 1. *Let $\sigma = (s_i)_{i=0}^{\infty}$ be a nonzero output sequence of a primitive n-stage NLFSR over $\mathbb{F}_q$, and let f be a nonzero polynomial over $\mathbb{F}_q$. Write f in the form*

$$f(x) = c\, x^a (x-1)^b f_1(x)^{e_1} \cdots f_s(x)^{e_s},$$

where $c \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, $f_1, \ldots, f_s$ are distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ none of which is equal to x or $x-1$, $e_1, \ldots, e_s$ are positive integers, a and b are nonnegative integers. Let $f_{i_1}, \ldots, f_{i_k}$ be all polynomials of $\{f_1, \ldots, f_s\}$ whose degrees divide n. Then the linear complexity $L(\tau)$ of the sequence $\tau = f(T)\sigma$ satisfies

$$L(\sigma) - \sum_{j=1}^{k} \deg(f_{i_j}) \leq L(\tau) \leq L(\sigma), \tag{4}$$

where $L(\sigma)$ denotes the linear complexity of σ and an empty sum has the value 0. In particular we have

$$L(\sigma) - \deg(f) \leq L(\tau) \leq L(\sigma). \tag{5}$$

Proof. By Lemma 4, the canonical factorization of m_σ in $\mathbb{F}_q[x]$ has the form $m_\sigma = \prod_{l=1}^{t} h_l$, where for all $l = 1, \ldots, t$, we have $\deg(h_l)$ divides n and $h_l(x) \neq x, x-1$. Hence $\gcd(m_\sigma, f)$ divides $g = \prod_{j=1}^{k} f_{i_j}$, where an empty product has the value 1. It follows that the degree of $m_\sigma / \gcd(m_\sigma, f)$ is lower bounded by $\deg(m_\sigma) - \deg(g)$ and upper bounded by $\deg(m_\sigma)$. An application of Lemma 3 completes the proof.

Corollary 1. *Let $\sigma \in V$ be as in Theorem 1. If the canonical factorization of the filter polynomial $f \in \mathbb{F}_q[x]$ over $\mathbb{F}_q$ contains only irreducible factors equal to x or $x-1$, or whose degrees do not divide n, then, for $\tau = f(T)\sigma$, we have $m_\tau = m_\sigma$, $L(\tau) = L(\sigma)$, and $\mathrm{per}(\tau) = \mathrm{per}(\sigma) = q^n - 1$.*

Proof. By the provisions above and Lemma 4, we infer that $\gcd(m_\sigma, f) = 1$. Therefore, according to Lemma 3, $m_\tau = m_\sigma$. This implies $L(\tau) = L(\sigma)$ and $\mathrm{per}(\tau) = \mathrm{ord}(m_\tau) = \mathrm{ord}(m_\sigma) = \mathrm{per}(\sigma) = q^n - 1$.

We are in particular interested in applying filter functions f whose degrees are smaller than the lengths of the respective NLFSR's. From a practical point of view this is the most interesting case (think of a hardware implementation of the shift register).

Corollary 2. *Let n be a prime and let σ be a nonzero output sequence of a primitive n-stage NLFSR over $\mathbb{F}_q$. If f is a nonzero polynomial over $\mathbb{F}_q$ with $\deg(f) < n$ and $\tau = f(T)\sigma$, then*

$$L(\tau) \geq L(\sigma) - \min(q-2, n-1).$$

If additionally, $f(c) \neq 0$ for all $c \in \mathbb{F}_q \setminus \{0,1\}$, then $m_\tau = m_\sigma$, so that $L(\tau) = L(\sigma)$ and $\mathrm{per}(\tau) = \mathrm{per}(\sigma) = q^n - 1$.

Proof. Since n is prime, the canonical factorization of m_σ in $\mathbb{F}_q[x]$ can contain only irreducible polynomials of degree 1 or n. Hence the assertion follows from Lemma 3 and Theorem 1.

Proposition 1. *Let $\sigma = (s_i)_{i=0}^{\infty}$ be a nonzero output sequence of a primitive n-stage NLFSR over $\mathbb{F}_q$. Let $f \in \mathbb{F}_q[x]$ be a nonzero polynomial with $\deg(f) < n$, and let $\tau = f(T)\sigma$. If the minimal polynomial m_σ is divisible by at least one primitive polynomial $h \in \mathbb{F}_q[x]$ of degree n, then $\mathrm{per}(\tau) = q^n - 1$.*

Proof. By Lemma 4, $m_\sigma = h_1 \cdots h_t$, where $h_1, \ldots, h_t \in \mathbb{F}_q[x]$ are distinct monic irreducible polynomials whose degrees divide n. It follows that $\mathrm{ord}(h_j)$ divides $q^n - 1$ for $1 \leq j \leq t$. Let us assume that h_1 is primitive and has degree n. Since $0 \leq \deg(f) < n$, $m_\tau = m_\sigma / \gcd(m_\sigma, f)$ still contains the primitive polynomial h_1. Let—after a possible rearrangement of factors—the canonical factorization of m_τ be given by $m_\tau = h_1 \cdots h_s$, where $s \leq t$. As $\mathrm{ord}(h_1) = q^n - 1$, we obtain $\mathrm{per}(\tau) = \mathrm{ord}(m_\tau) = \mathrm{lcm}(\mathrm{ord}(h_1), \ldots, \mathrm{ord}(h_s)) = q^n - 1$.

Corollary 3. *Let $\sigma, \tau \in V$ and $f \in \mathbb{F}_q[x]$ be as in Proposition 1. If the linear complexity of σ satisfies $L(\sigma) \geq q^n - 1 - \phi(q^n - 1)$, where ϕ is Euler's function, then $\mathrm{per}(\tau) = q^n - 1$.*

Proof. The rth cyclotomic polynomial over $\mathbb{F}_q$ has degree $\phi(r)$ and, for $r = q^n - 1$, is the product of all (monic) primitive polynomials in $\mathbb{F}_q[x]$ having degree n (see [10]). Thus, if $L(\sigma) = \deg(m_\sigma) \geq r - \phi(r)$, at least one primitive polynomial $h \in \mathbb{F}_q[x]$ of degree n must be present in the canonical factorization of m_σ over $\mathbb{F}_q$.

4 Distribution properties

Let σ be a nonzero output sequence of a primitive NLFSR over $\mathbb{F}_q$, and let f be a nonzero polynomial over $\mathbb{F}_q$. We will show that up to a slight aberration for the zero element the elements of $\mathbb{F}_q$ are equidistributed in the sequence $\tau = f(T)\sigma$, provided that the degree of the filter polynomial is not too large. Moreover, all possible strings of elements of $\mathbb{F}_q$ up to a certain length (which depends on the degree of the applied filter polynomial f) appear almost equally often within a full portion of the period of τ. If $f(x) = x^e g(x)$ with $e \geq 0$ and $g \in \mathbb{F}_q[x]$ with $g(0) \neq 0$, then the sequence $f(T)\sigma$ is a shifted version of the sequence $g(T)\sigma$. Therefore, w.l.o.g. we can restrict our attention to filter polynomials f which are not divisible by x.

Theorem 2. *Let $\sigma = (s_i)_{i=0}^{\infty}$ a nonzero output sequence of a primitive n-stage NLFSR over $\mathbb{F}_q$. Let $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$ and $0 \leq \deg(f) = k \leq n-1$. Let $\tau = (t_i)_{i=0}^{\infty} = f(T)\sigma$. For $1 \leq m \leq n-k$ and $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}_q^m$, let $N(\mathbf{b})$ be the number of $i \in \{0, 1, \ldots, r-1\}$ for which $(t_i, t_{i+1}, \ldots, t_{i+m-1}) = \mathbf{b}$. Then*

$$N(\mathbf{b}) = \begin{cases} q^{n-m} & \text{for } \boldsymbol{b} \neq \boldsymbol{0}, \\ q^{n-m} - 1 & \text{for } \boldsymbol{b} = \boldsymbol{0}. \end{cases}$$

Proof. By assumption, $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ with $a_0 a_k \neq 0$. Thus

$$t_i = a_0 s_i + a_1 s_{i+1} + \cdots + a_k s_{i+k} \qquad \text{for } i = 0, 1, \ldots.$$

Let $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}_q^m$ be fix. Consider the system of m linear equations in n unknowns $x_0, x_1, \ldots, x_{n-1}$, given by

$$\sum_{j=0}^{k} a_j x_{j+h} = b_{h+1}, \qquad h = 0, 1, \ldots, m-1. \tag{6}$$

Let A be the matrix of coefficients of the corresponding homogeneous system of linear equations, so that

$$A = \begin{pmatrix} a_0 & a_1 & \ldots & a_k & 0 & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_k & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \ddots & & \ddots & & & \vdots \\ 0 & 0 & \ldots & a_0 & a_1 & \ldots & a_k & \ldots & 0 \end{pmatrix}.$$

Then A is an $m \times n$ matrix over $\mathbb{F}_q$ of rank m, since $a_0 \neq 0$. If $\mathbf{b} \neq \mathbf{0}$ then the augmented matrix $A' = (A, \mathbf{b}^{\mathrm{t}})$, which is the $m \times (n+1)$ matrix whose first n columns are the columns of the matrix A and whose last column is the transpose of $\mathbf{b}$, has also rank m. Hence the system of linear equations in (6) has q^{n-m} distinct solution vectors $(x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n$.

If $\mathbf{b} = \mathbf{0}$, then the zero vector of $\mathbb{F}_q^n$ is one of the q^{n-m} solution vectors of the system (6). As i runs through $0, 1, \ldots, r-1$, all nonzero n-tuples occur among $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{r-1} \in \mathbb{F}_q^n$, so that $N(\mathbf{0}) = q^{n-m} - 1$. If $\mathbf{b} \neq \mathbf{0}$, then all q^{n-m} solution vectors of (6) are nonzero and thus occur among $\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{r-1}$, so that $N(\mathbf{b}) = q^{n-m}$.

5 A running key generator

Consider k primitive binary NLFSR's of pairwise relatively prime lengths $n_1, \ldots, n_k$. For each $j = 1, \ldots, k$, the jth NLFSR is endowed with a modifiable linear feedforward logic described by a certain collection C_j of binary polynomials of degrees less than n_j. The key loading algorithm has to perform two tasks:

1. It loads each of the k NLFSR's with a nonzero initial state vector;
2. For each $j = 1, \ldots, k$, it selects a filter polynomial f_j from the set C_j.

Let σ_j be the binary sequence the jth NLFSR would produce, due to the chosen initial state vector, without filtering. Then $\tau_j = f_j(T)\sigma_j$ is the sequence after applying the chosen filter polynomial f_j. The linearly filtered sequences $\tau_1, \ldots, \tau_k$ are combined termwise by a Boolean combining function $F : \mathbb{F}_2^k \to \mathbb{F}_2$ to produce the keystream $\omega = F(\tau_1, \ldots, \tau_k)$.

The internal state of the running key generator at time t consists of the binary contents of the $n_1 + \cdots + n_k$ memory cells of the whole shift register bundle. The output function of the running key generator depends on the k-tuple $(f_1, \ldots, f_k)$ of filter polynomials that were chosen during key loading. A well designed key loading algorithm guarantees that each possible combination $(f_1, \ldots, f_k)$ of the filter polynomials will occur with the same probability if the secret key is chosen at random from the uniform distribution. The number N of different combinations of the filter polynomials is given by

$$N = \prod_{j=1}^{k} |C_j|,$$

where $|C_j|$ denotes the cardinality of the set C_j. Thus the running key generator has N different output functions and, therefore, can generate N translation distinct keystream sequences. The latter is a desired property by an information theoretical analysis of keystream generators carried out by Jansen [6, Chap. 7]. The rest of this section is devoted to the derivation of the minimal polynomial of the keystream sequence ω.

First we recall some results of Selmer [20, Chap. 4]. Let $f, g, \ldots, h \in \mathbb{F}_q[x]$ be nonconstant polynomials without multiple roots in their respective splitting fields over $\mathbb{F}_q$ and with nonzero constant terms. Then $f \vee g \vee \cdots \vee h$ is defined to be the monic polynomial whose roots are the distinct products $\alpha\beta\cdots\gamma$, where α is a root of f, β a root of g, and γ a root of h. The polynomial $f \vee g \vee \cdots \vee h$ is again a polynomial over the ground field $\mathbb{F}_q$. This follows from the fact that all conjugates (over $\mathbb{F}_q$) of a root of $f \vee g \vee \cdots \vee h$ are roots of $f \vee g \vee \cdots \vee h$.

Lemma 5. *Let $f, g, \ldots, h \in \mathbb{F}_q[x]$ be polynomials over $\mathbb{F}_q$ without multiple roots and with nonzero constant terms. The polynomial $f \vee g \vee \cdots \vee h \in \mathbb{F}_q[x]$ is irreducible if and only if the polynomials $f, g, \ldots, h$ are all irreducible and of pairwise relatively prime degrees. In this case,*

$$\deg(f \vee g \vee \cdots \vee h) = \deg(f)\deg(g)\cdots\deg(h).$$

If $\sigma, \tau, \ldots, \upsilon$ are periodic sequences in V with irreducible minimal polynomials $f, g, \ldots, h \in \mathbb{F}_q[x]$ of pairwise relatively prime degrees and with $f(0)g(0)\cdots h(0) \neq 0$, then $f \vee g \vee \cdots \vee h$ is the minimal polynomial of the product sequence $\sigma\tau\cdots\upsilon$.

Proof. See Selmer [20, Chap. 4].

Lemma 6. *For each $j = 1, \ldots, k$, let σ_j be a periodic sequence in V with minimal polynomial $m_j \in \mathbb{F}_q[x]$. If the polynomials $m_1, \ldots, m_k$ are pairwise relatively prime, then the minimal polynomial of the sum $\sigma = \sigma_1 + \cdots + \sigma_k$ is equal to the product $m_1 \cdots m_k$. Conversely, let σ be a periodic sequence in V whose minimal polynomial $m \in \mathbb{F}_q[x]$ is the product of pairwise relatively prime monic polynomials $m_1, \ldots, m_k \in \mathbb{F}_q[x]$. Then, for each $j = 1, \ldots, k$, there exists a uniquely determined periodic sequence σ_j with minimal polynomial $m_j \in \mathbb{F}_q[x]$ such that $\sigma = \sigma_1 + \cdots + \sigma_k$.*

Proof. A proof of the first part of the lemma can be found on page 426 in Lidl and Niederreiter [10]. To prove the second part, let $h/m \in \mathbb{F}_q(x)$ be the generating function of σ in the sense of Lemma 1. Let

$$\frac{h}{m} = \frac{h_1}{m_1} + \cdots + \frac{h_k}{m_k} \tag{7}$$

be the partial fraction decomposition of h/m. By the comments following Lemma 1, $\deg(h) < \deg(m)$ and $\gcd(h, m) = 1$. This implies $\deg(h_j) < \deg(m_j)$ and $\gcd(h_j, m_j) = 1$ for $1 \leq j \leq k$. The rational functions h_j/m_j correspond to uniquely determined periodic sequences $\sigma_j \in V$ with minimal polynomials m_j. Equation (7) implies that $\sigma = \sigma_1 + \cdots + \sigma_k$.

Lemma 7. *Let $S, T, \ldots, U$ be pairwise relatively prime integers greater than 1. Let $\sigma = (s_n)_{n=0}^{\infty}$, $\tau = (t_n)_{n=0}^{\infty}$, $\ldots$, $\upsilon = (u_n)_{n=0}^{\infty}$ be periodic binary sequences of periods $\mathrm{per}(\sigma) = 2^S - 1$, $\mathrm{per}(\tau) = 2^T - 1$, $\ldots$, $\mathrm{per}(\upsilon) = 2^U - 1$, respectively. Assume that the canonical factorizations over $\mathbb{F}_2$ of the minimal polynomials of $\sigma, \tau, \ldots, \upsilon$ are*

$$m_\sigma = \prod_{i=1}^{s} f_i, \qquad m_\tau = \prod_{j=1}^{t} g_j, \qquad \ldots, \qquad m_\upsilon = \prod_{k=1}^{u} h_k. \tag{8}$$

Then the minimal polynomial of the product sequence $\sigma\tau\cdots\upsilon = (s_n t_n \cdots u_n)_{n=0}^{\infty}$ is given by

$$m_{\sigma\tau\cdots\upsilon} = \prod_{i=1}^{s} \prod_{j=1}^{t} \cdots \prod_{k=1}^{u} (f_i \vee g_j \vee \cdots \vee h_k). \tag{9}$$

In fact, (9) represents the canonical factorization of the minimal polynomial of $\sigma\tau\cdots\upsilon$ over $\mathbb{F}_2$.

Proof. It suffices to carry out the details of the proof for the product of two sequences σ and τ. The general statement then follows by induction. Consider the canonical factorization of the minimal polynomials m_σ and m_τ in (8). By

hypothesis, $r = \mathrm{per}(\sigma) = 2^S - 1$ which implies that m_σ divides $x^r - 1$. Recall that $x(x^r - 1) = x^{2^S} - x \in \mathbb{F}_2[x]$ is the product of all irreducible binary polynomials whose degrees divide S. It follows that the irreducible factors $f_1, \ldots, f_s$ are distinct and that $\deg(f_i)$ divides S for $1 \le i \le s$. Similarly, the irreducible polynomials $g_1, \ldots, g_t$ are distinct and $\deg(g_j)$ divides T for $1 \le j \le t$. Furthermore, the first-degree irreducible polynomial $p(x) = x$ does not occur among the polynomials $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$. By Lemma 6, the sequences σ and τ possess unique representations

$$\sigma = \sum_{i=1}^{s} \sigma_i \quad \text{and} \quad \tau = \sum_{j=1}^{t} \tau_j,$$

where σ_i is a binary periodic sequence with minimal polynomial f_i for $1 \le i \le s$, and τ_j is a binary periodic sequence with minimal polynomial g_j for $1 \le j \le t$. It follows that

$$\sigma\tau = \sum_{i=1}^{s} \sum_{j=1}^{t} \sigma_i \tau_j.$$

By hypothesis, $\gcd(S, T) = 1$. It follows that for each $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, t\}$, the corresponding irreducible polynomials f_i and g_j have relatively prime degrees. Invoking Lemma 5, we conclude that for each $i \in \{1, \ldots, s\}$ and $j \in \{1, \ldots, t\}$, the sequence $\sigma_i\tau_j$ has the irreducible minimal polynomial $f_i \vee g_j \in \mathbb{F}_2[x]$.

As will be shown below, the irreducible polynomials $f_i \vee g_j$, $1 \le i \le s$, $1 \le j \le t$, are distinct. Another application of Lemma 6 shows that the minimal polynomial of $\sigma\tau$ has the form

$$m_{\sigma\tau} = \prod_{i=1}^{s} \prod_{j=1}^{t} (f_i \vee g_j). \tag{10}$$

It remains to show that the polynomials $f_i \vee g_j$, $1 \le i \le s$, $1 \le j \le t$, are distinct. To see this, let f_i and f_i' be any two factors from the canonical factorization of m_σ, and let g_j and g_j' be any two factors from the canonical factorization of m_τ. Assume to the contrary that the two irreducible polynomials $f_i \vee g_j$ and $f_i' \vee g_j'$ are equal. Note that two irreducible polynomials over the finite field $\mathbb{F}_q$ are equal if and only if they have a common root (in some extension field of $\mathbb{F}_q$). Let γ be a common root of the polynomials $f_i \vee g_j$ and $f_i' \vee g_j'$. Then we can write γ in the form

$$\gamma = \alpha\beta = \alpha'\beta', \tag{11}$$

where α, β, α', and β' are roots of the polynomials f_i, g_j, f_i', and g_j', respectively. Since α is a root of the irreducible polynomial f_i, we have $\alpha \in \mathbb{F}_{2^{\deg(f_i)}}$, which is a subfield of $\mathbb{F}_{2^S}$, as $\deg(f_i)$ divides S. Similarly, we conclude that $\alpha' \in \mathbb{F}_{2^S}$ and $\beta, \beta' \in \mathbb{F}_{2^T}$. From (11) we obtain $\alpha/\alpha' = \beta'/\beta$. Clearly, $\alpha/\alpha' \in \mathbb{F}_{2^S}$ and $\beta'/\beta \in \mathbb{F}_{2^T}$. Since S and T are relatively prime we have $\mathbb{F}_{2^S} \cap \mathbb{F}_{2^T} = \mathbb{F}_2$, so that $\alpha/\alpha' = \beta'/\beta = 1$. Hence $\alpha = \alpha'$ and $\beta = \beta'$. This implies $f_i = f_i'$ and $g_j = g_j'$.

Theorem 3. *Let $\sigma_1, \ldots, \sigma_k$ be nonzero output sequences of $k \geq 1$ primitive binary NLFSR's of pairwise relatively prime lengths $n_1, \ldots, n_k$. Let the canonical factorization of the minimal polynomial of σ_j over $\mathbb{F}_2$ be given by*

$$m_{\sigma_j} = \prod_{i_j=1}^{d_j} h_{i_j} \qquad \text{for } 1 \leq j \leq k.$$

Let $F : \mathbb{F}_2^k \to \mathbb{F}_2$ be an arbitrary Boolean combining function with algebraic normal form

$$F(x_1, \ldots, x_k) = a_0 + \sum_{1 \leq i \leq k} a_i x_i + \sum_{1 \leq i < j \leq k} a_{ij} x_i x_j + \cdots + a_{12\ldots k} x_1 x_2 \cdots x_k.$$

Consider the linearly filtered sequences $\tau_j = f_j(T)\sigma_j$ for $1 \leq j \leq k$ and the combined sequence $\omega = F(\tau_1, \ldots, \tau_k)$. If for $j = 1, \ldots, k$, the applied filter polynomial $f_j \in \mathbb{F}_2[x]$ does not contain any irreducible factors $\neq x, x-1$ whose degrees divide n_j, then the minimal polynomial of ω is given by

$$\begin{aligned} m_\omega = (x-1)^{a_0} &\left(\prod_{i_1=1}^{d_1} h_{i_1} \right)^{a_1} \left(\prod_{i_2=1}^{d_2} h_{i_2} \right)^{a_2} \cdots \left(\prod_{i_k=1}^{d_k} h_{i_k} \right)^{a_k} \\ &\cdot \left(\prod_{i_1=1}^{d_1} \prod_{i_2=1}^{d_2} (h_{i_1} \vee h_{i_2}) \right)^{a_{12}} \cdots \left(\prod_{i_{k-1}=1}^{d_{k-1}} \prod_{i_k=1}^{d_k} (h_{i_{k-1}} \vee h_{i_k}) \right)^{a_{k-1,k}} \\ &\cdots \left(\prod_{i_1=1}^{d_1} \prod_{i_2=1}^{d_2} \cdots \prod_{i_k=1}^{d_k} (h_{i_1} \vee h_{i_2} \vee \cdots \vee h_{i_k}) \right)^{a_{12\cdots k}}. \end{aligned} \tag{12}$$

Proof. By Corollary 1, $m_{\tau_j} = m_{\sigma_j}$ for $1 \leq j \leq k$. We have

$$\omega = a_0 + \sum_{1 \leq i \leq k} a_i \tau_i + \sum_{1 \leq i < j \leq k} a_{ij} \tau_i \tau_j + \cdots + a_{12\ldots k} \tau_1 \tau_2 \ldots \tau_k. \tag{13}$$

For each summand we know the corresponding minimal polynomial from Lemma 7. It remains to show that the minimal polynomials of the individual summands are pairwise relatively prime. Lemma 6 then yields the presented formula for the minimal polynomial m_ω.

Consider any two different summands in the sum in (13). There exists at least one τ_l that appears in one of the two summands but not in the other. Consider the minimal polynomials of the two summands. By Corollary 1, we have $m_{\tau_l} = m_{\sigma_l}$, and therefore

$$m_{\tau_l} = \prod_{i_l=1}^{d_l} h_{i_l}.$$

According to Lemma 4, the irreducible factors h_{i_l} satisfy: (i) $\deg(h_{i_l})$ divides n_l; (ii) $\deg(h_{i_l}) \geq 2$. Consider the minimal polynomials of the two summands. By Lemma 5, and since $\gcd(n_i, n_j) = 1$ for $i \neq j$, it follows that all irreducible factors in the canonical factorization of the minimal polynomial of the summand that does not contain τ_l have degrees relatively prime to n_l. On the other hand, each irreducible polynomial in the canonical factorization of the minimal polynomial of the summand that contains τ_l is of the form $(h_{(\cdot)} \vee \cdots \vee h_{i_l})$, and its degree is a multiple of $\deg(h_{i_l})$, by Lemma 5. Therefore, the degree of the polynomial cannot be relatively prime to n_l. It follows that the minimal polynomials of any two summands in (13) are relatively prime.

By taking the degrees of both sides in the formula (12), we can express the linear complexity of ω in terms of the linear complexities of the sequences $\sigma_1, \ldots, \sigma_k$. A typical value for the linear complexity of a nonzero output sequence of a primitive binary n-stage NLFSR seems to be the maximum possible value $2^n - 2$. This is supported by extensive computer investigations of ours.

Corollary 4. *Assume that the underlying primitive binary NLFSR's are such that the linear complexities of the nonzero output sequences σ_j attain the maximum possible values $L(\sigma_j) = 2^{n_j} - 2$ for $1 \leq j \leq k$. Assume that the jth NLFSR is initialized with any nonzero vector of $\mathbb{F}_2^{n_j}$. Let for each j, the applied filter polynomial run through all $2^{n_j} - 1$ nonzero polynomials of $\mathbb{F}_2[x]$ with $0 \leq \deg(f_j) < n_j$. Then the linear complexities of the corresponding possible output sequences ω of the running key generator all satisfy*

$$F(2^{n_1} - n_1 - 1, \ldots, 2^{n_k} - n_k - 1) \leq L(\omega) \leq F(2^{n_1} - 2, \ldots, 2^{n_k} - 2).$$

Proof. By Corollary 3, we have $\mathrm{per}(\tau_j) = 2^{n_j} - 1$ for all nonzero $f_j \in \mathbb{F}_2[x]$ with $0 \leq \deg(f_j) < n_j$, $1 \leq j \leq k$. By Theorem 1, we have $L(\tau_j) \geq L(\sigma_j) - \deg(f_j) \geq 2^{n_j} - n_j - 1$. The assertion now follows from Theorem 3.

6 Maximum order complexity

A sequence that is obtained by randomly choosing a string of r elements of $\mathbb{F}_q$ which is then repeated ad infinitum to produce a periodic sequence of $\mathbb{F}_q^\infty$ is expected to have maximum order complexity $2\lceil \log_q(r) \rceil$ (see Jansen [6]). By computer calculations we found that the mean value of the maximum order complexity of linearly filtered nonzero output sequences of primitive binary n-stage NLFSR's is close to the ideal value $2n$, provided that the applied filter polynomial f satisfies $2 \leq \deg(f) < n$.

Table 1 displays for a primitive binary NLFSR of length 12 the maximum order complexity values of its linearly filtered sequences $\tau = f(T)\sigma$. The applied filter polynomial $f \in \mathbb{F}_2[x]$ ranges over all binary polynomials with $f(0) = 1$ and $\deg(f) \leq 11$. Table 2 gives the mean values and standard deviations of the maximum order complexities of linearly filtered nonzero output sequences of primitive binary NLFSR's of different lengths. The lengths n of the NLFSR's

vary in the range $4 \leq n \leq 23$. For $n = 4, 5, 6$ all binary primitive NLFSR's were taken into account. For each larger value of n, at least 300 randomly selected primitive binary NLFSR's were considered. In each considered n-stage NLFSR the applied filter polynomial f runs through all binary nonzero polynomials with $\deg(f) \leq n - 1$.

$\deg(f)$	Min.	Max.	Average	$\deg(f)$	Min.	Max.	Average
0	12	12	12.000	6	20	30	23.375
1	20	20	20.000	7	19	31	23.578
2	19	27	23.000	8	20	30	23.352
3	21	30	24.750	9	19	34	23.203
4	19	29	23.750	10	19	35	23.322
5	19	28	23.375	11	19	34	23.332

Table 1. Minimum, maximum, and average values of the maximum order complexity for linearly filtered nonzero output sequences of a primitive binary 12-stage NLFSR.

n	Mean value	Std. Dev.	n	Mean value	Std. Dev.
4	5.99	1.64	14	27.64	2.91
5	8.16	2.28	15	29.65	2.63
6	10.55	2.36	16	31.83	3.06
7	12.77	2.39	17	33.58	2.40
8	15.03	2.95	18	35.57	2.30
9	17.37	3.82	19	37.80	2.72
10	19.35	3.08	20	40.18	2.80
11	21.42	2.75	21	42.42	3.39
12	23.62	3.10	22	43.42	2.01
13	25.74	3.40	23	45.49	2.26

Table 2. Mean value and standard deviation of the maximum order complexity for linearly filtered nonzero output sequences of primitive binary n-stage NLFSR's.

7 Acknowledgement

The authors thank the anonymous referees for their useful comments and suggestions. Special thanks go to Lothrop Mittenthal and Johannes Mykkeltveit for insightful discussions at the WCC 2005 Workshop in Bergen.

References

1. T. van Aardenne-Ehrenfest and N. G. de Bruijn: Circuits and trees in oriented linear graphs, *Simon Steven* **28**, 203–217 (1951).
2. Z.-D. Dai and J.-H. Yang: Linear complexity of periodically repeated random sequences, *Advances in Cryptology — EUROCRYPT '91* (D. W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, pp. 168–175, Springer-Verlag, 1991.
3. A. Fúster-Sabater and P. Caballero-Gil: On the linear complexity on nonlinearly filtered PN-sequences, *Advances in Cryptology — ASIACRYPT '94* (J. Pieprzyk and R. Safavi-Naini, eds.), Lecture Notes in Computer Science, vol. 917, pp. 80–90, Springer-Verlag, 1995.
4. S. W. Golomb: *Shift Register Sequences*, Aegean Park Press, Laguna Hills, CA, 1982.
5. E. J. Groth: Generation of binary sequences with controllable complexity, *IEEE Trans. Inform. Theory* **IT-17**, 288–296 (1971).
6. C. J. A. Jansen: *Investigations On Nonlinear Streamcipher Systems: Construction and Evaluation Methods*, Ph.D. Thesis, Technical University of Delft, Delft, 1989.
7. E. Key: An analysis of the structure and complexity of nonlinear binary sequence generators, *IEEE Trans. Inform. Theory* **IT-22**, 732–736 (1976).
8. D. Laksov: Linear recurring sequences over finite fields, *Math. Scand.* **16**, 181–196 (1965).
9. C. C. Y. Lam and G. Gong: A lower bound for the linear span of filtering sequences, Workshop Record of *The State of the Art of Stream Ciphers* (Brugge, Oct. 2004), pp. 220–233.
10. R. Lidl and H. Niederreiter: *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, Reading, Mass., 1983. (Now Cambridge Univ. Press.)
11. J. L. Massey and S. Serconek: A Fourier transform approach to the linear complexity of nonlinearly filtered sequences, *Advances in Cryptology — CRYPTO '94* (Y. G. Desmedt, ed.), Lecture Notes in Computer Science, vol. 839, pp. 332–340, Springer-Verlag, 1994.
12. W. Meidl and H. Niederreiter: On the expected value of the linear complexity and the k-error linear complexity of periodic sequences, *IEEE Trans. Inform. Theory* **48**, 2817–2825 (2002).
13. J. Mykkeltveit: Nonlinear recurrences and arithmetic codes, *Information and Control* **33**, 193-209 (1977).
14. J. Mykkeltveit, M.-K. Siu, and P. Tong: On the cycle structure of some nonlinear shift register sequences, *Information and Control* **43**, 202–215 (1979).
15. H. Niederreiter: Cryptology—The mathematical theory of data security, *Prospects of Mathematical Science* (T. Mitsui, K. Nagasaka, and T. Kano, eds.), pp. 189–209, World Sci. Pub., Singapore, 1988.
16. H. Niederreiter: *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NFS Regional Conference Series in Applied Mathematics, vol. 63, SIAM, Philadelphia, PA, 1992.
17. H. Niederreiter: Sequences with almost perfect linear complexity profile, *Advances in Cryptology — EUROCRYPT '87* (D. Chaum and W. L. Price, eds.), Lecture Notes in Computer Science, vol. 304, pp. 37–51, Springer-Verlag, Berlin, 1985.
18. K. G. Paterson: Root counting, the DFT and the linear complexity of nonlinear filtering, *Designs, Codes and Cryptography* **14**, 247–259 (1998).
19. R. A. Rueppel: *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.

20. E. S. Selmer: *Linear Recurrence Relations over Finite Fields*, Department of Mathematics, Univ. of Bergen, 1966.
21. T. Siegenthaler, R. Forré, and A. W. Kleiner: Generation of binary sequences with controllable complexity and ideal r-tupel distribution, *Advances in Cryptology — EUROCRYPT '87* (D. Chaum and W.L. Price, eds.), Lecture Notes in Computer Science, vol. 304, pp. 15–23, Springer-Verlag, 1988.
22. M. Willett: The minimum polynomial for a given solution of a linear recursion, *Duke Math. J.* **39**, 101–104 (1972).