A General Lower Bound for the Linear Complexity of the Product of Shift-Register Sequences

Rainer Göttfert and Harald Niederreiter

Institute for Information Processing
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Vienna, Austria

E-mail: goet@qiinfo.oeaw.ac.at
nied@qiinfo.oeaw.ac.at

Abstract: The determination of the linear complexity of the product of two shift-register sequences is a basic problem in the theory of stream ciphers. We present for the first time a lower bound for the linear complexity of the product of two shift-register sequences in the general case. Moreover, we provide information on the minimal polynomial of such a product.

1 Introduction

An important tool for the assessment of the suitability of keystreams for their use in stream ciphers is the concept of linear complexity (see Rueppel [7]). For a (linear feedback) shift-register sequence σ, its *linear complexity* $L(\sigma)$ can be informally described as the length of the shortest (linear feedback) shift register that generates σ. More precisely, $L(\sigma)$ is defined as the degree of the *minimal polynomial* of σ. Recall that the minimal polynomial of σ is, by definition, the monic polynomial of largest degree that divides all characteristic polynomials of σ (compare with [5, Chapter 6]). The minimal polynomial of σ can also be described in terms of the generating function of σ (see Lemma 1 below).

Practical methods for the generation of keystreams employ various combinations of shift-register sequences (see again [7]). To determine the linear complexity of such combined shift-register sequences, it essentially suffices to analyze the behavior of shift-register sequences under elementary operations such as termwise addition and multiplication. If this behavior is known, then the effect of general Boolean combining functions can also be predicted. Since the treatment of the termwise sum of shift-register sequences is comparatively easy, the attention of researchers has focused on the linear complexity of the (termwise) product of shift-register sequences (see e.g. [1], [3], [4], [8]). In this paper we set ourselves the more ambitious task of providing information about the minimal polynomial of a product of shift-register sequences; naturally, this yields, in particular, results on the linear complexity of such a product. By determining

either the minimal polynomial itself or a factor of it, we obtain either an exact formula or a lower bound for the linear complexity of a product of shift-register sequences. Clearly, lower bounds on the linear complexity of keystreams are of great cryptographic relevance.

Throughout this paper, $\mathbb{F}_q$ denotes a fixed finite field of order q and characteristic p. For an arbitrary field F and a monic polynomial $f \in F[x]$ let $M_F(f)$ be the set of all shift-register sequences in F with minimal polynomial f. If $F = \mathbb{F}_q$, then for simplicity we write $M(f)$ instead of $M_F(f)$. We denote the minimal polynomial of a shift-register sequence σ in F by $m_\sigma \in F[x]$.

With this notation, the basic problem considered in this paper can be formulated as follows: given monic polynomials $f, g \in \mathbb{F}_q[x]$, provide as much information as possible about the minimal polynomial $m_{\sigma\tau} \in \mathbb{F}_q[x]$ of the product sequence $\sigma\tau = (s_n t_n)_{n=0}^{\infty}$ in $\mathbb{F}_q$, where $\sigma = (s_n)_{n=0}^{\infty} \in M(f)$ and $\tau = (t_n)_{n=0}^{\infty} \in M(g)$. Zierler and Mills [9] determined a polynomial $Z(f,g) \in \mathbb{F}_q[x]$ that is divisible by all minimal polynomials $m_{\sigma\tau}$ with $\sigma \in M(f)$ and $\tau \in M(g)$. As a counterpart of this result, we obtain in Theorem 1 a polynomial $A(f,g) \in \mathbb{F}_q[x]$ that divides all polynomials $m_{\sigma\tau}$ with $\sigma \in M(f)$ and $\tau \in M(g)$. Thus, we have the divisibility relations

$$(1) \qquad A(f,g) \mid m_{\sigma\tau} \mid Z(f,g) \qquad \text{for all } \sigma \in M(f) \text{ and } \tau \in M(g).$$

Certain polynomials $f, g \in \mathbb{F}_q[x]$ satisfy $A(f,g) = Z(f,g)$, and in this case (1) implies

$$m_{\sigma\tau} = A(f,g) = Z(f,g) \qquad \text{for all } \sigma \in M(f) \text{ and } \tau \in M(g),$$

which means that the minimal polynomial of the product sequence $\sigma\tau$ is uniquely determined by the minimal polynomials of the individual sequences σ and τ (compare with Theorem 2).

2 The Definition of $A(f,g)$

To describe the polynomial $A(f,g)$, we need the following definition. We write $\mathbb{N}$ for the set of positive integers and $\mathbb{N}_0$ for the set of nonnegative integers.

Definition. For $a, b \in \mathbb{N}$ we define $a \vee b$ as the maximum value of $i+j+1$ such that the binomial coefficient $\binom{i+j}{i}$ is not divisible by p, where $i, j \in \mathbb{N}_0$ with $0 \le i \le a-1$ and $0 \le j \le b-1$.

From this definition we immediately obtain

$$\max(a,b) \le a \vee b \le a+b-1.$$

Furthermore, we have

$$a \vee b = a+b-1 \Leftrightarrow \binom{a+b-2}{a-1} \not\equiv 0 \bmod p.$$

Let f and g be nonconstant monic polynomials over $\mathbb{F}_q$. Without a serious loss of generality, we can assume that $f(0) \neq 0$ and $g(0) \neq 0$ (compare with [5, p. 222]). Let E be the splitting field of fg over $\mathbb{F}_q$, let $\alpha_1, \ldots, \alpha_r \in E$ be the distinct roots of f with corresponding multiplicities $a_1, \ldots, a_r$, and let $\beta_1, \ldots, \beta_s \in E$ be the distinct roots of g with corresponding multiplicities $b_1, \ldots, b_s$. We put

$$C = \{(i,j) \in \mathbb{N}^2 : 1 \leq i \leq r,\ 1 \leq j \leq s\}.$$

Let $\gamma_1, \ldots, \gamma_t$ be the distinct elements among the products $\alpha_i \beta_j$ with $(i,j) \in C$. We decompose C into the pairwise disjoint subsets

$$C_d = \{(i,j) \in C : \alpha_i \beta_j = \gamma_d\} \qquad \text{for } 1 \leq d \leq t.$$

We now define

$$A(f,g)(x) = \prod_{d=1}^{t}{}^{*} (x - \gamma_d)^{e_d} \in \mathbb{F}_q[x], \tag{2}$$

where the asterisk indicates that the product is extended only over those d satisfying the following property: the set C_d contains a pair (i,j) for which $\binom{a_i+b_j-2}{a_i-1} \not\equiv 0 \bmod p$ and $a_k \vee b_l < a_i \vee b_j$ for all $(k,l) \in C_d$ with $(k,l) \neq (i,j)$. Via this uniquely determined pair $(i,j) \in C_d$ we then define

$$e_d = a_i \vee b_j = a_i + b_j - 1.$$

As usual, an empty product, which may occur in (2), has the value 1.

3 The Main Result

The following theorem yields for the first time a general lower bound for the linear complexity of the product of shift-register sequences.

Theorem 1. *Let $f, g \in \mathbb{F}_q[x]$ be nonconstant monic polynomials with $f(0)g(0) \neq 0$ as in Section 2 and let $\sigma \in M(f)$ and $\tau \in M(g)$. Then the minimal polynomial $m_{\sigma\tau}$ of the product sequence $\sigma\tau$ is divisible by the polynomial $A(f,g)$ in (2). In particular, for the linear complexity $L(\sigma\tau)$ of $\sigma\tau$ we have*

$$L(\sigma\tau) \geq \deg(A(f,g)).$$

For the proof of Theorem 1 we need two lemmas. The first lemma is taken from [6, Lemma 2]. We adopt the convention $\deg(0) = -\infty$.

Lemma 1. *A sequence $(s_n)_{n=0}^{\infty}$ in a field F is a shift-register sequence with minimal polynomial $m \in F[x]$ if and only if the generating function $\sum_{n=0}^{\infty} s_n x^{-n-1}$ of $(s_n)_{n=0}^{\infty}$ is a rational function of the form h/m with $h \in F[x]$, $\deg(h) < \deg(m)$, and $\gcd(h,m) = 1$.*

Lemma 2. *Let F be an arbitrary field of characteristic p, let $\alpha, \beta \in F$ with $\alpha\beta \neq 0$, and let $a, b \in \mathbb{N}$. Then for all $\sigma \in M_F((x-\alpha)^a)$ and $\tau \in M_F((x-\beta)^b)$ the minimal polynomial $m_{\sigma\tau} \in F[x]$ of the product sequence $\sigma\tau$ has the form*

$$m_{\sigma\tau}(x) = (x - \alpha\beta)^c \tag{3}$$

with a $c \in \mathbb{N}_0$ that may depend on σ and τ and satisfies $0 \leq c \leq a \vee b$. Furthermore, we have $c = a + b - 1$ if and only if $\binom{a+b-2}{a-1} \not\equiv 0 \bmod p$.

Proof. The proof of [3, Lemma 3] provides also a proof of this lemma. □

Remark 1. If σ runs through $M_F((x-\alpha)^a)$ and τ runs through $M_F((x-\beta)^b)$, then not all possible values of c have to appear in (3). However, if $\binom{a+b-2}{a-1} \equiv 0 \bmod p$, then the "extreme values" $c = 0$ and $c = a \vee b$ are always attained. This can be shown by refining the proof of [3, Lemma 3]; compare with [2, Satz 5.1].

Proof of Theorem 1. Let σ and τ be as in the theorem and let E be the splitting field of fg over $\mathbb{F}_q$. If we view σ and τ as sequences in E, then they can be written in the form

$$\sigma = \sum_{i=1}^{r} \sigma_i \qquad \text{and} \qquad \tau = \sum_{j=1}^{s} \tau_j$$

with $\sigma_i \in M_E((x-\alpha_i)^{a_i})$ for $1 \leq i \leq r$ and $\tau_j \in M_E((x-\beta_j)^{b_j})$ for $1 \leq j \leq s$. Therefore

$$\sigma\tau = \sum_{(i,j)\in C} \sigma_i \tau_j . \tag{4}$$

Let the rational function $h/m_{\sigma\tau} \in \mathbb{F}_q(x) \subseteq E(x)$ be the generating function of $\sigma\tau$ in reduced form. By Lemmas 1 and 2, the generating function of $\sigma_i\tau_j$ has the reduced form

$$\frac{h_{ij}(x)}{(x - \alpha_i\beta_j)^{c_{ij}}},$$

where $0 \leq c_{ij} \leq a_i \vee b_j$ and $h_{ij} \in E[x]$ with $\deg(h_{ij}) < c_{ij}$. Then, by turning to generating functions, we see that (4) leads to the identity

$$\frac{h(x)}{m_{\sigma\tau}(x)} = \sum_{(i,j)\in C} \frac{h_{ij}(x)}{(x - \alpha_i\beta_j)^{c_{ij}}}$$

in the rational function field $E(x)$. Using the partition of C into $C_1, \ldots, C_t$, this identity can be written as

$$\frac{h(x)}{m_{\sigma\tau}(x)} = \sum_{d=1}^{t} \sum_{(i,j)\in C_d} \frac{h_{ij}(x)}{(x - \gamma_d)^{c_{ij}}}. \tag{5}$$

To show that $A(f,g)$ divides $m_{\sigma\tau}$, we consider

$$\sum_{(i,j)\in C_d} \frac{h_{ij}(x)}{(x-\gamma_d)^{c_{ij}}} \tag{6}$$

for a fixed d satisfying the following property: there exists a pair $(i,j) \in C_d$ for which $\binom{a_i+b_j-2}{a_i-1} \not\equiv 0 \bmod p$ and $a_k \vee b_l < a_i \vee b_j$ for all $(k,l) \in C_d$ with $(k,l) \neq (i,j)$. For this pair (i,j) we then get by Lemma 2,

$$c_{ij} = a_i + b_j - 1 = a_i \vee b_j = e_d$$

and

$$c_{kl} \leq a_k \vee b_l < e_d \qquad \text{for all } (k,l) \in C_d \text{ with } (k,l) \neq (i,j).$$

Consequently, the rational function in (6) has the form

$$\frac{a(x)(x-\gamma_d)+b(x)}{(x-\gamma_d)^{e_d}}$$

with $a(x), b(x) \in E[x]$ and $b(x)$ not divisible by $x-\gamma_d$. In other words, this rational function is in reduced form. From (5) we can then infer that $m_{\sigma\tau}(x)$ contains the factor $(x-\gamma_d)^{e_d}$. Altogether, we obtain that the polynomial $A(f,g)$ in (2) divides $m_{\sigma\tau}$ in $E[x]$.

In fact, $A(f,g)$ is even a polynomial over the ground field $\mathbb{F}_q$. This can be shown by verifying that if γ is a root of $A(f,g)$ of multiplicity c, then every conjugate of γ relative to $\mathbb{F}_q$ is also a root of $A(f,g)$ of multiplicity c. The verification uses some nontrivial results of the theory of finite extensions of fields, but is otherwise straightforward; compare with [2, pp. 56–57]. □

4 Further Results and Remarks

Remark 2. In our notation the Zierler-Mills polynomial $Z(f,g)$ associated with f and g can be described as

$$Z(f,g)(x) = \prod_{d=1}^{t} (x-\gamma_d)^{z_d} \in \mathbb{F}_q[x],$$

where

$$z_d = \max_{(i,j)\in C_d} (a_i \vee b_j) \qquad \text{for } 1 \leq d \leq t.$$

We mention that our definition of $a \vee b$ for $a, b \in \mathbb{N}$ is equivalent to the one in [9]. The right-hand side of (5) can be written as a rational function with denominator $Z(f,g)$ since $c_{ij} \leq a_i \vee b_j$, and so it follows that $m_{\sigma\tau}$ is always a divisor of $Z(f,g)$. So as a byproduct we obtain an essential result of [9].

Theorem 2. *Let $f, g \in \mathbb{F}_q[x]$ be as in Theorem 1 and suppose that every d with $1 \le d \le t$ satisfies the following property: C_d contains a pair (i,j) for which $\binom{a_i+b_j-2}{a_i-1} \not\equiv 0 \bmod p$ and $a_k \vee b_l < a_i \vee b_j$ for all $(k,l) \in C_d$ with $(k,l) \neq (i,j)$. With this pair $(i,j) \in C_d$ we put $e_d = a_i + b_j - 1$. Then for all $\sigma \in M(f)$ and $\tau \in M(g)$ the minimal polynomial of $\sigma\tau$ is given by*

$$m_{\sigma\tau}(x) = \prod_{d=1}^{t} (x - \gamma_d)^{e_d} \in \mathbb{F}_q[x].$$

In particular, for all $\sigma \in M(f)$ and $\tau \in M(g)$ the linear complexity of $\sigma\tau$ has the value

$$L(\sigma\tau) = \sum_{d=1}^{t} e_d.$$

Proof. Under the given conditions we have

$$A(f,g)(x) = Z(f,g)(x) = \prod_{d=1}^{t} (x - \gamma_d)^{e_d},$$

and so the theorem follows from the divisibility relations in (1). □

Theorem 3. *Let $f, g \in \mathbb{F}_q[x]$ be as in Theorem 1 and suppose that the rs products $\alpha_i\beta_j$ with $(i,j) \in C$ are distinct. Put*

$$C^{(0)} = \left\{(i,j) \in C : \binom{a_i + b_j - 2}{a_i - 1} \equiv 0 \bmod p\right\}$$

and $C^{(1)} = C \setminus C^{(0)}$. Then for all $\sigma \in M(f)$ and $\tau \in M(g)$ the minimal polynomial of $\sigma\tau$ has the form

$$m_{\sigma\tau}(x) = \prod_{(i,j)\in C^{(0)}} (x - \alpha_i\beta_j)^{c_{ij}} \cdot \prod_{(i,j)\in C^{(1)}} (x - \alpha_i\beta_j)^{a_i+b_j-1},$$

where the $c_{ij} \in \mathbb{N}_0$ may depend on σ and τ and satisfy $0 \le c_{ij} \le a_i \vee b_j$ for all $(i,j) \in C^{(0)}$.

Proof. Since the products $\alpha_i\beta_j$ with $(i,j) \in C$ are distinct, each subset C_d in the partition of C is a singleton. Therefore, the polynomial in (2) is given by

$$A(f,g)(x) = \prod_{(i,j)\in C^{(1)}} (x - \alpha_i\beta_j)^{a_i+b_j-1}, \tag{7}$$

and for the Zierler-Mills polynomial we get

$$Z(f,g)(x) = \prod_{(i,j)\in C^{(0)}} (x - \alpha_i\beta_j)^{a_i \vee b_j} \cdot \prod_{(i,j)\in C^{(1)}} (x - \alpha_i\beta_j)^{a_i+b_j-1}.$$

Consequently, the desired result follows from (1). □

Note that both Theorem 2 and Theorem 3 contain [3, Theorem 1] as a special case.

Remark 3. Consider the special sequences $\sigma = (s_n)_{n=0}^{\infty}$ and $\tau = (t_n)_{n=0}^{\infty}$ whose terms are given by

$$s_n = \sum_{i=1}^{r} \binom{n}{a_i - 1} \alpha_i^n \qquad \text{and} \qquad t_n = \sum_{j=1}^{s} \binom{n + b_j - 1}{b_j - 1} \beta_j^n \qquad \text{for } n = 0, 1, \ldots.$$

With the method employed in the proof of [3, Lemma 3], one can show that $\sigma \in M(f)$ and $\tau \in M(g)$ and that, under the conditions of Theorem 3, the minimal polynomial $m_{\sigma\tau}$ is equal to the polynomial $A(f, g)$ in (7). Theorem 2 shows also that we can have $m_{\sigma\tau} = A(f, g)$ and that $m_{\sigma\tau} = Z(f, g)$ is possible as well. Therefore, the polynomials $A(f, g)$ and $Z(f, g)$ are in general best possible with respect to (1).

References

[1] Golić, J. Dj.: On the linear complexity of functions of periodic GF(q) sequences, *IEEE Trans. Inform. Theory* **35**, 69–75 (1989).

[2] Göttfert, R.: Produkte von Schieberegisterfolgen, Ph.D. Dissertation, Univ. of Vienna, 1993.

[3] Göttfert, R., and Niederreiter, H.: On the linear complexity of products of shift-register sequences, *Advances in Cryptology — EUROCRYPT '93* (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. **765**, pp. 151–158, Springer-Verlag, Berlin, 1994.

[4] Herlestam, T.: On functions of linear shift register sequences, *Advances in Cryptology — EUROCRYPT '85* (F. Pichler, ed.), Lecture Notes in Computer Science, vol. **219**, pp. 119–129, Springer-Verlag, Berlin, 1986.

[5] Lidl, R., and Niederreiter, H.: *Introduction to Finite Fields and Their Applications*, Cambridge University Press, Cambridge, 1986.

[6] Niederreiter, H.: 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, 1988.

[7] Rueppel, R. A.: Stream ciphers, *Contemporary Cryptology: The Science of Information Integrity* (G. J. Simmons, ed.), pp. 65–134, IEEE Press, New York, 1992.

[8] Rueppel, R. A., and Staffelbach, O. J.: Products of linear recurring sequences with maximum complexity, *IEEE Trans. Inform. Theory* **33**, 124–131 (1987).

[9] Zierler, N., and Mills, W. H.: Products of linear recurring sequences, *J. Algebra* **27**, 147–157 (1973).