ON DECIMATION OF LINEAR RECURRING SEQUENCES

Jovan Dj. Golić
Information Security Research Centre, Queensland University of Technology
GPO Box 2434, Brisbane Qld 4001, Australia
School of Electrical Engineering, University of Belgrade
(*Submitted March 1994*)

1. INTRODUCTION

The problem of obtaining a linear recursion for a decimated sequence in terms of the linear recursion for the original finite field sequence has been studied extensively in the literature either from a mathematical point of view or in connection with various applications mostly having to do with high-speed parallel generation of linear recurring sequences. A survey of such applications, mainly in spread spectrum communications and cryptography, can be found in [4]. The special case of sequences satisfying primitive or irreducible polynomials was treated in [10], [7], and [3], whereas the general case was settled in [2]. Alternative approaches to the general case were given in [5], [6], [8], and [4]. Recently, the results from [2] have been extended to arbitrary fields [1] by using the results on products of linear recurring sequences from [11]. Unlike the method from [2], which is based on the decimation of individual sequences, the method from [1] deals with vector spaces of sequences.

In this paper we develop a novel approach that enables us to determine the minimum generating polynomial of decimated sequences over an arbitrary field in a simple and self-contained way. This is achieved starting from a new characterization of this polynomial and by using some facts from the general field theory, without invoking any results on product sequences. Some new properties of decimated sequences are also pointed out.

2. PRELIMINARIES

Let F be an arbitrary field, let $s = \{s(t)\}_{t=0}^{\infty}$ denote a sequence over F, and let $f(x) = \sum_{i=0}^{n} c_i x^i$ be a polynomial over F such that $f(0) \neq 0$. Then s is called a *linear recurring sequence* satisfying f if

$$\sum_{i=0}^{n} c_i s(t+i) = 0, \quad t \geq 0. \tag{1}$$

Let $L_F(f)$ or simply $L(f)$ denote the set of all s over F that satisfy f. If the degree of f is n, then $L(f)$ is an n-dimensional vector space over F which is closed under the translate operator $Ts = \{s(t+1)\}_{t=0}^{\infty}$. For every linear recurring sequence s over F, the unique monic polynomial g over F of lowest degree satisfied by s is called the *minimum polynomial* of s and s is called a *regular sequence* of g, see [2]. The minimum polynomial of a finite set of linear recurring sequences is defined analogously and is equal to the least common multiple of the minimum polynomials of individual sequences, see [10].

Given a sequence s over F and a positive integer d, the *decimation* of s by d, $s^{(d)}$, is defined by $s^{(d)}(t) = s(td)$, $t \geq 0$. Analogously, given a set S of sequences over F, the decimation of S by d, $S^{(d)}$, is defined by $S^{(d)} = \{s^{(d)} : s \in S\}$. Besides, given a nonnegative integer τ, the *translate* of s by τ, $s_{(\tau)}$, is defined by $s_{(\tau)}(t) = s(t+\tau)$, $t \geq 0$, that is, $s_{(\tau)} = T^{\tau}s$.

The set $L^{(d)}(f)$ is a vector space over F generated by the set $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{n-1}$ of decimated sequences obtained from the successive translates of any regular sequence s of f of degree n. Since $L^{(d)}(f)$ is closed under the translate operator, $L^{(d)}(f) = L(h)$, where h is the minimum polynomial of the set $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{n-1}$. Moreover, since every sequence from $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{n-1}$ is a translate of a sequence from $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$ and since the minimum polynomial of a translate divides the minimum polynomial of the original sequence, h is also the minimum polynomial of the set $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$. This set is important for the high-speed parallel generation of s, because s can be obtained by interleaving the corresponding decimated sequences generated at d times lower speed than s.

For a finite field F, Duvall and Mortick [2] obtained the minimum polynomial h in terms of f, d, and the characteristic of F, by considering the decimations of sequences from an appropriate basis of $L(f)$. Recently, by using the results from [11] on product sequences, Buck and Zierler [1] have developed a new method which enabled them to extend the result [2] to arbitrary fields. Polynomials with multiple roots in both [2] and [1] are dealt with in relatively involved ways, which is also the case with inseparable polynomials in [1]. In the next section, we show how the minimum polynomial of decimated sequences can be derived in a new way that is both simple and compact. Instead of the results on product sequences, it is based on some facts from the general field theory and treats the inseparable and separable polynomials in a unified way.

3. MINIMUM POLYNOMIAL OF DECIMATED SEQUENCES

Our objective is to derive the minimum polynomial of the set $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$ of d sequences obtained from the decimation by d of d successive translates of an arbitrary linear recurring sequence s over a field F. To this end, first note that the original sequence s can be obtained by interleaving the considered d decimated sequences. Second, for an arbitrary polynomial g over F such that $g(0) \neq 0$, $L(g(x^d))$ is the set of all the sequences obtained by interleaving d members of $L(g(x))$, see [1]. Therefore, for an arbitrary polynomial g over F, $g(0) \neq 0$, if s is a regular sequence of a polynomial f over F, $f(0) \neq 0$, then $f(x) | g(x^d)$ holds if and only if the decimated sequences $s_{(\tau)}^{(d)}, 0 \leq \tau \leq d-1$, all satisfy g. In view of the definition of minimum polynomials, we thus obtain the following simple characterization of the minimum polynomial of the considered decimated sequences.

Theorem 1: Let f be a monic polynomial over F, $f(0) \neq 0$, let d be a positive integer, and let s be a regular sequence of f. The minimum polynomial of the set of decimated sequences $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$ is then equal to the unique monic polynomial g over F of minimum degree such that $f(x) | g(x^d)$. •

Since the minimum polynomial established in Theorem 1 depends only of f and d, we adopt the notation $f_{(d)}$. It remains to find out an explicit characterization of $f_{(d)}$. We proceed in three steps by proving the following lemmas.

Lemma 1: Let $f = \text{l.c.m.}(f_1, f_2)$, where f_1 and f_2 are monic polynomials over F, $f_1(0) \neq 0$, $f_2(0) \neq 0$. Then $f_{(d)} = \text{l.c.m.}(f_{1,(d)}, f_{2,(d)})$. •

Proof: Let $h = \text{l.c.m.}(f_{1,(d)}, f_{2,(d)})$. We use the fact, already noted in the proof of Theorem 1, that $a(x) | b(x^d) \Leftrightarrow a_{(d)} | b$, for arbitrary monic polynomials a and b over F, $a(0) \neq 0$, $b(0) \neq 0$.

Accordingly, for an arbitrary monic polynomial g over F, $g(0) \neq 0$, it follows that $f(x) | g(x^d) \Leftrightarrow f_i(x) | g(x^d)$, $i = 1, 2 \Leftrightarrow f_{i,(d)} | g$, $i = 1, 2 \Leftrightarrow h | g$. Hence, $h = f_{(d)}$. •

Lemma 2: Let f be a monic and irreducible polynomial over F, $f(0) \neq 0$, and let α be any root of f in a splitting field E of f. Then $f_{(d)}$ is the minimum polynomial of α^d over F. •

Proof: First, note that the minimum polynomial h of α^d over F exists because E is an algebraic extension of F. We employ the well-known result, see [9], that the minimum polynomial of an element γ algebraic over F must divide every polynomial g over F such that $g(\gamma) = 0$. It suffices to prove that $f(x) | g(x^d) \Leftrightarrow g(\alpha^d) = 0$ for an arbitrary monic polynomial g over F, $g(0) \neq 0$. Namely, by the definition of the minimum polynomial, it then follows that $f_{(d)} = h$. The implication "$\Rightarrow$" is clear because α is then a root of $g(x^d)$. The implication "$\Leftarrow$" is true because, if α is a root of $g(x^d)$, then the minimum polynomial of α, which is f, must divide $g(x^d)$. •

Lemma 3: Let $f = g^r$, where g is a monic and irreducible polynomial over F, $g(0) \neq 0$, and r is a positive integer. If F has characteristic $p = 0$, then $f_{(d)} = g_{(d)}^r$. If F has characteristic $p > 0$, $d = kp^c$, $p \nmid k$, and $e \geq 0$ is the exponent of inseparability of g, then $f_{(d)} = g_{(d)}^{\lceil r/p^{\max(c-e,0)} \rceil}$, $\lceil z \rceil$ denoting the smallest integer not smaller than a real number z. •

Proof: We first prove that $f_{(d)} = g_{(d)}^t$ for some positive integer t. Note that by Lemma 2 $g_{(d)}$ is irreducible. Assume that $f_{(d)} = a g_{(d)}^t$, where $g_{(d)} \nmid a$. Then the minimality of $f_{(d)}$ implies that $g^r(x) | a(x^d) g_{(d)}^t(x^d)$ and $g^r(x) \nmid g_{(d)}^t(x^d)$. Since g is irreducible, then $g(x) | a(x^d)$; hence, $g_{(d)} | a$, which contradicts the assumption.

To determine t, we should analyze the multiplicities of the roots of g, $g_{(d)}$, and $g_{(d)}(x^d)$. We use some well-known facts from the general field theory (see [9], Ch. II, §1-6). If the characteristic p of F is zero, then both g and $g_{(d)}$ are separable and the roots of g, $g_{(d)}$, and $g_{(d)}(x^d)$ are all simple. Then $t = r$. If F has characteristic $p > 0$, $d = kp^c$, $p \nmid k$, and $e \geq 0$ is the exponent of inseparability of g (g is separable if $e = 0$), then all the roots of g have multiplicity p^e. Note that the exponent of inseparability of g is equal to the minimum nonnegative integer i such that α^{p^i} is separable over F, where α is is a root of g in a splitting field of g. Therefore, the exponent of inseparability of the minimum polynomial $g_{(d)}$ of α^d is $\max(e - c, 0)$; hence, all the roots of $g_{(d)}$ have multiplicity $p^{\max(e-c,0)}$. Finally, all the roots of $g_{(d)}(x^d)$ have p^c times larger multiplicity than the roots of $g_{(d)}$, that is, $p^{\max(e,c)}$. Then t is the minimum positive integer j such that $rp^e \leq jp^{\max(e,c)}$. •

Consequently, in view of Theorem 1, Lemmas 1, 2, and 3 result in the following characterization of the minimum polynomial of decimated sequences.

Theorem 2: Let f be a monic polynomial over F, $f(0) \neq 0$, that factors as $f = \prod_{i=1}^m f_i^{r_i}$, where f_i are distinct monic and irreducible polynomials, let d be a positive integer, and let s be a regular sequence of f. Then the minimum polynomial of the set of decimated sequences $\{s_{(\tau)}^{(d)}\}_{\tau=0}^{d-1}$ is given by

$$f_{(d)} = \text{l.c.m.}\left(f_{i,(d)}^{t_i} : 1 \leq i \leq m\right), \tag{2}$$

where $f_{i,(d)}$ is the minimum polynomial of α_i^d over F, α_i being any root of f_i in a splitting field of f, $t_i = r_i$ if F has characteristic zero, and $t_i = \lceil r_i / p^{\max(c-e_i,0)} \rceil$ if F has characteristic $p > 0$, $d = kp^c$, $p \nmid k$, and $e_i \geq 0$ is the exponent of inseparability of f_i, $1 \leq i \leq m$. •

Theorem 2 specifies $f_{(d)}$ as the minimum polynomial of a set of d decimated sequences rather than the set of all the decimated sequences, which is interesting for parallel generation of linear recurring sequences. As is shown in Section 2, $L^{(d)}(f) = L(f_{(d)})$ also holds, so that expression (2) is equivalent to the one from [1]. However, our characterization is slightly different because of the unified treatment of inseparable and separable polynomials and because of the different treatment of the root multiplicities.

Finally, we also prove the following properties yielding a necessary and sufficient condition for the minimum polynomial of a decimated sequence to depend only on the minimum polynomial of the original sequence, which is interesting for cryptographic applications. Note that the proof makes no use of Theorem 2.

Proposition: Let f be a monic polynomial over F, $f(0) \neq 0$, and let d be a positive integer. Then the decimation by d defines a homomorphism of $L(f)$ onto $L(f_{(d)})$; hence, $\deg f_{(d)} \leq \deg f$. If and only if $\deg f_{(d)} = \deg f$, then the decimation by d defines an isomorphism of $L(f)$ onto $L(f_{(d)})$. Furthermore, if $\deg f_{(d)} = \deg f$, then the minimum polynomial of $s^{(d)}$ is $f_{(d)}$ for every regular sequence s of f. •

Proof: The proof of the first assertion is straightforward. The second assertion directly follows from the well-known fact in the theory of vector spaces (see [9], Ch. I, §21), that a homomorphism of a finite-dimensional vector space onto another vector space is an isomorphism if and only if their dimensions are equal (otherwise, the dimension of the image vector space is strictly smaller than the dimension of the original one). As for the third assertion, assume that there exists a regular sequence s of f such that $s^{(d)}$ is a regular sequence of h, where h is a proper factor of $f_{(d)}$. From the definition of $f_{(d)}$, it then follows that the polynomial $g(x) = \text{g.c.d.}(f(x), h(x^d))$ is a proper factor of f such that $g_{(d)} = h$. Then $L^{(d)}(g) = L(h)$, which means that there exists another sequence $s' \in L(f)$ different from s such that $s^{(d)} = s'^{(d)}$. Therefore, the decimation is not an isomorphism and the second assertion then implies that $\deg f_{(d)} < \deg f$. •

ACKNOWLEDGMENT

The author is grateful to an anonymous referee for useful comments.

REFERENCES

1. M. Buck & N. Zierler. "Decimations of Linear Recurring Sequences." In *Proceedings of Golombfest*, Oxnard, California, May 1992.
2. P. F. Duvall & J. C. Mortick. "Decimation of Periodic Sequences." *SIAM J. Appl. Math.* **21** (1971):367-72.
3. S. W. Golomb. *Shift Register Sequences*. San Francisco: Holden-Day, 1967.
4. C. G. Günther. "Parallel Generation of Recurring Sequences." In Advances in Cryptology-EUROCRYPT '89. *Lect. Notes in Comp. Sci.* **434** (1990):503-22.
5. H. Niederreiter. "Some New Cryptosystems Based on Feedback Shift Register Sequences." *Math. J. Okayama Univ.* **30** (1988):121-49.

6. H. Niederreiter. "A Simple and General Approach to the Decimation of Feedback Shift-Register Sequences." *Probl. of Control and Inform. Theory* **17** (1988):327-31.
7. E. S. Selmer. *Linear Recurrence Relations Over Finite Fields.* Lecture Notes, University of Bergen, Norway, 1966.
8. B. Smeets. "Some Results on Linear Recurring Sequences." Ph.D. Dissertation, University of Lund, Sweden, 1987.
9. O. Zarriski & P. Samuel. *Commutative Algebra.* Vol. I. Princeton: D. Van Nostrand, 1958.
10. N. Zierler. "Linear Recurring Sequences." *J. Soc. Indust. Appl. Math.* **7** (1959):31-48.
11. N. Zierler & W. H. Mills. "Products of Linear Recurring Sequences." *J. Algebra* **27** (1973): 147-57.

AMS Classification Numbers: 11B37, 12E05, 94A60

GENERALIZED PASCAL TRIANGLES AND PYRAMIDS:
THEIR FRACTALS, GRAPHS, AND APPLICATIONS

by Dr. Boris A. Bondarenko
Associate member of the Academy of Sciences of the Republic of Uzbekistan, Tashkent

Translated by Professor Richard C. Bollinger
Penn State at Erie, The Behrend College

This monograph was Wrst published in Russia in 1990 and consists of seven chapters, a list of 406 references, an appendix with another 126 references, many illustrations and specific examples. Fundamental results in the book are formulated as theorems and algorithms or as equations and formulas. For more details on the contents of the book, see *The Fibonacci Quarterly* **31.1** (1993):52.

The translation of the book is being reproduced and sold with the permission of the author, the translator, and the "FAN" Edition of the Academy of Science of the Republic of Uzbekistan. The book, which contains approximately 250 pages, is a paperback with a plastic spiral binding. The price of the book is $31.00 plus postage and handling where postage and handling will be $6.00 if mailed anywhere in the United States or Canada, $9.00 by surface mail or $16,00 by airmail elsewhere. A copy of the book can be purchased by sending a check make out to **THE FIBONACÇI ASSOCIATION** for the appropriate amount along with a letter requesting a copy of the book to: **MR. RICHARD S. VINE, SUBSCRIPTION MANAGER, THE FIBONACCI ASSOCIATION, SANTA CLARA UNIVERSITY, SANTA CLARA, CA 95053.**