Linear Complexity of Periodic Sequences: A General Theory*

James L. Massey[1] and Shirlei Serconek[2]**

[1] Signal and Information Processing Laboratory
Swiss Federal Institute of Technology
ETH-Zentrum, CH-8092 Zürich (massey@isi.ee.ethz.ch)
[2] Instituto de Matematica e Fisica - IMF
Universidade Federal de Goias - UFG
Departamento de Matematica, Cx Postal 131
74001-970 Goiania GO, BRAZIL

Abstract. The linear complexity of an N-periodic sequence with components in a field of characteristic p, where $N = np^\nu$ and $\gcd(n, p) = 1$, is characterized in terms of the n^{th} roots of unity and their multiplicities as zeroes of the polynomial whose coefficients are the first N digits of the sequence. Hasse derivatives are then introduced to quantify these multiplicities and to define a new generalized discrete Fourier transform that can be applied to sequences of arbitrary length N with components in a field of characteristic p, regardless of whether or not $\gcd(N, p) = 1$. This generalized discrete Fourier transform is used to give a simple proof of the validity of the well-known Games-Chan algorithm for finding the linear complexity of an N-periodic binary sequence with $N = 2^\nu$ and to generalize this algorithm to apply to N-periodic sequences with components in a finite field of characterisitic p when $N = p^\nu$. It is also shown how to use this new transform to study the linear complexity of Hadamard (i.e., component-wise) products of sequences.

Keywords: *discrete Fourier transform, DFT, Games-Chan algorithm, Hadamard product, Hasse derivative, hyperderivative, linear complexity, stream ciphers*

1 Introduction

The main purpose of this paper is to provide a convenient framework for the study of the linear complexity of periodic sequences with an arbitrary period. In particular when the sequence is an N-periodic sequence with components in a field of characteristic p and $N = np^\nu$ where $\gcd(n, p) \neq 1$, we seek a formulation

* This document includes corrections of some typos in the printed paper, which appears in *Advances in CryptologyCRYPTO'96* (Ed. N. Koblitz), Lecture Notes in Computer Science No. 1109. New York: Springer, 1996, pp. 358-371.

** This work was done while the author was on leave at the ETH Zürich from CEPESC, Cx Postal 02976, Brasília, DF, BRASIL, CEP 70610-200.

that is as convenient as that for the usually studied case when $\gcd(N,p) = 1$. In Section 2, we give such a formulation in terms of the n^{th} roots of unity and their multiplicities as zeroes of the polynomial whose coefficients are the first N digits of the sequence. This leads naturally to the use of the Hasse derivative as described in Section 3 to characterize linear complexity.

Another purpose of this paper is to introduce a new generalization of the discrete Fourier transform that admits application to sequences of arbitrary length N. This is done in Section 4, where it is further shown that the linear complexity of an N-periodic sequence with components in a finite field of characteristic p is equal to the appropriately defined "weight" of its generalized discrete Fourier transform.

To illustrate the usefulness of the approach in this paper, we give in Section 5.1 a simple proof of the validity of the well-known Games-Chan algorithm for finding the linear complexity of an N-periodic binary sequence with $N = 2^\nu$, and we generalize this algorithm to apply to N-periodic sequences with components in a finite field of characterisitic p and $N = p^\nu$. Finally, in Section 5.2, we show how our techniques can be used to study the linear complexity of Hadamard products of sequences.

2 Linear Complexity of Periodic Sequences

The *linear complexity*, $\mathcal{L}(\tilde{\mathbf{s}})$, of the semi-infinite F- ary sequence $\tilde{\mathbf{s}} = s_0, s_1, s_2, \cdots$, where each s_i lies in the field F, is the smallest nonnegative integer L for which there exist coefficients $c_1, c_2, \cdots, c_L$ in F such that

$$s_j + c_1 s_{j-1} + \cdots + c_L s_{j-L} = 0 \text{ for all } \mathrm{j} \geq \mathrm{L}$$

or, equivalently, such that

$$P(D) = (s_0 + s_1 D + s_2 D^2 + \cdots)C(D), \tag{1}$$

is a polynomial of degree strictly less than L where $C(D) = 1 + c_1 D + c_2 D^2 + \cdots + c_L D^L$. In engineering terms, $\mathcal{L}(\tilde{\mathbf{s}})$ is the length L of the shortest linear feedback shift- register (LFSR) that can generate $\tilde{\mathbf{s}}$ when the first L digits of $\tilde{\mathbf{s}}$ are initially loaded in the register; the polynomial $C(D)$ is called the *connection polynomial* of the LFSR.

Suppose now that the sequence $\tilde{\mathbf{s}}$ is N-periodic, i.e., $s_i = s_{i+N}$ for all $i \geq 0$. Then the formal power series $s_0 + s_1 D + s_2 D^2 + \cdots$ can be written

$$s_0 + s_1 D + s_2 D^2 + \cdots = s^N(D)(1 + D^N + D^{2N} + \cdots)$$

where $s^N(D) = s_0 + s_1 D + s_2 D^2 + \cdots + s_{N-1} D^{N-1}$ is the polynomial of degree less than N determined by $\mathbf{s}^N = [s_0, s_1, \cdots, s_{N-1}]$, and hence

$$(s_0 + s_1 D + s_2 D^2 + \cdots)(1 - D^N) = s^N(D).$$

Multiplying by $1 - D^N$ in (1) thus gives $P(D)(1 - D^N) = s^N(D)C(D)$, which ensures that $\deg(P(D)) < \deg(C(D))$. It follows that the necessary and sufficient

condition for $C(D) = 1+c_1D+c_2D^2+\cdots+c_LD^L$, with coefficients in F and with $c_L \neq 0$, to be the connection polynomial of the shortest LFSR that generates $\tilde{\mathbf{s}}$, and hence for $L = \deg(C(D))$ to be the linear complexity of $\tilde{\mathbf{s}}$, is that

$$s^N(D)C(D) = P(D)(1 - D^N) \tag{2}$$

where $P(D)$ is a polynomial satisfying

$$\gcd(P(D), C(D)) = 1. \tag{3}$$

The zeroes of $1 - D^N$ are N^{th} roots of unity by definition and in general lie in some extension field E of F. When a primitive N^{th} root of unity [i.e., one which is not also an n^{th} root of unity for some n with $1 \leq n < N$] does not exist, then the distinct zeroes of $1 - D^N$ will have multiplicity greater than 1. Suppose now that γ is a zero of $1 - D^N$ with positive multiplicity k. It follows from (2) and (3) that γ is a zero of $C(D)$ with positive multiplicity m if and only if γ is a zero of $s^N(D)$ with multiplicity $\mu = k - m \geq 0$. But (2) and (3) also imply that γ can be a zero of $C(D)$ only when γ is a zero of $1 - D^N$, and hence we have proved the following useful lemma.

Lemma 1. *Let $C(D)$ be the connection polynomial of the shortest LFSR that generates the F-ary N-periodic sequence $\tilde{\mathbf{s}}$. Then a zero, γ, of $1 - D^N$ with positive multiplicity k is a zero of $C(D)$ with positive multiplicity m if and only if γ is a zero of $s^N(D)$ with multiplicity μ such that $0 \leq \mu < k$, in which case $m = k - \mu$. Moreover, $C(D)$ has no zeroes other than those determined in this manner.*

Consider now the case where the field F has characteristic p so that N may be written as $N = np^\nu$ where $\gcd(n, p) = 1$. Then there exists a primitive n^{th} root of unity, α, in some extension field of F so that $\alpha^i, i = 0, 1, \cdots, n-1$, are the n distinct roots of unity. Moreover,

$$1 - D^N = (1 - D^n)^{p^\nu}$$

and hence α^i is a zero of $1 - D^N$ with multiplicity p^ν for $i = 0, 1, \cdots, n-1$. Using these facts together with Lemma 1 yields the following result.

Proposition 2. *Let $C(D)$ be the connection polynomial of the shortest LFSR that generates the F-ary N-periodic sequence $\tilde{\mathbf{s}}$, where F is a field of prime characteristic p and where $N = np^\nu$ with $\gcd(n, p) = 1$, and let α be a primitive n^{th} root of unity in F or some extension of F. Then α^i, where $0 \leq i < n$, is a zero of $C(D)$ with positive multiplicity m_i if and only if α^i is a zero of $s^N(D)$ with multiplicity μ_i less than p^ν, in which case $m_i = p^\nu - \mu_i$. Moreover, these are all the zeroes of $C(D)$ so that the linear complexity of $\tilde{\mathbf{s}}$ is $\mathcal{L}(\tilde{\mathbf{s}}) = m_0 + m_1 + \cdots + m_{n-1}$.*

Note that $\mu_i = 0$ or $m_i = 0$ in the proposition indicates that α^i is *not* a zero of $s^N(D)$ or $C(D)$, respectively. The usefulness of this proposition is that it characterizes the linear complexity of the N-periodic sequence $\tilde{\mathbf{s}}$ entirely in terms

of the multiplicities of the n^{th} roots of unity as zeroes of $s^N(D)$, a polynomial directly available from the sequence $\tilde{\mathbf{s}}$. Of course, as the lemma states, this is equivalent to determining the multiplicities of the n^{th} roots of unity as zeroes of $C(D)$ or, again equivalently, of the reciprocal polynomial of $C(D)$, which is often called the *characteristic polynomial* of the sequence. Determining the linear complexity of an N-periodic sequence by "counting zeroes" of its characteristic polynomial is a technique that has been used by many authors, cf. [8], [13] and particularly [15], p. 78, but the emphasis on "counting zeroes" in $s^N(D)$ appears to be novel. To proceed further with such zero-counting, we require the derivative described in the next section.

3 Hasse Derivatives and Hasse Matrices

Let $F[D]$ denote the ring of polynomials in the indeterminate D with coefficients in a field F and let $a(D) = \sum_i a_i D^i$ be a polynomial in $F[D]$. The j^{th} *formal derivative* of $a(D)$ is defined to be the polynomial

$$\begin{aligned} a^{(j)}(D) &= \sum_i i(i-1)\cdots(i-j+1)a_i D^{i-j} \\ &= j! \sum_i \binom{i}{j} a_i D^{i-j}\,. \end{aligned}$$

The usefulness of the formal derivative in a field of prime characteristic p is greatly limited by the fact that $a^{(j)}(D) = 0$ for all $j \geq p$ because then $j! = 0$. Of greater utility in such fields is the j^{th} *Hasse derivative* [7] (sometimes called the j^{th} *hyperderivative* [9], and, particularly when extended to rational functions, the *Hasse-Teichmüller derivative* [6], [16]), which is defined as

$$a^{[j]}(D) = \sum_i \binom{i}{j} a_i D^{i-j}\,.$$

Note that $a^{(j)}(D) = (j!)a^{[j]}(D)$ and hence it is always true that $a^{(1)}(D) = a^{[1]}(D)$. Hasse derivatives in any field have the same connection to repeated factors of a polynomial as do formal derivatives in fields of characteristic 0, namely (cf. [3]):

Theorem 3. *If $h(D)$ is irreducible in $F[D]$ with $h^{(1)}(D) \neq 0$ and if m is any positive integer, then $[h(D)]^m$ divides $a(D)$ if and only if $h(D)$ divides $a(D)$ and its first $m-1$ Hasse derivatives.*

Remark. If F is a finite field or a field of characteristic 0, then every $h(D)$ that is irreducible in $F[D]$ satisfies $h^{(1)}(D) \neq 0$.

Invoking Theorem 3, we immediately obtain the following corollary of Proposition 2.

Corollary 4. *Let $\tilde{\mathbf{s}}$ be an F-ary N-periodic sequence, where F is a finite field of characteristic p and where $N = np^\nu$ with $\gcd(n,p) = 1$, and let α be a primitive n^{th} root of unity in F or some extension of F. Then the linear complexity of $\tilde{\mathbf{s}}$ is $\mathcal{L}(\tilde{\mathbf{s}}) = m_0 + m_1 + \cdots + m_{n-1}$ where*

$$m_i = \begin{cases} 0, & \text{if } s^N(\alpha^i) = s^{N[1]}(\alpha^i) = \cdots = s^{N[p^\nu - 1]}(\alpha^i) = 0 \\ p^\nu - \min\{j : s^{N[j]}(\alpha^i) \neq 0\}, & \text{otherwise.} \end{cases}$$

Example 1. Consider the binary (i.e., $F = \mathrm{GF}(2)$) 12-periodic sequence $\tilde{\mathbf{s}}$ with $\mathbf{s}^{12} = [0,0,1,0,1,0,1,0,0,0,0,0]$. Then $N = 12$ and $p = 2$, which gives $n = 3$ and $\nu = 2$. Taking α as a primitive third root of unity in an extension of GF(2) requires that α be a zero of $x^2 + x + 1$ and hence that $\alpha^2 = \alpha + 1$. From the sequence $\mathbf{s}^{12}$ we obtain immediately the polynomial $s^{12}(D) = D^2 + D^4 + D^6$. Taking Hasse derivatives gives the $p^\nu - 1 = 3$ polynomials required to be considered in Corollary 4, namely $s^{12[1]}(D) = 0$, $s^{12[2]}(D) = 1 + D^4$, and $s^{12[3]}(D) = 0$. Direct subsitution of α^i in these polynomials gives

$$\begin{aligned} s^{12}(1) &= 1 \\ s^{12}(\alpha) = 0,\ s^{12[1]}(\alpha) &= 0,\ s^{12[2]}(\alpha) = 1 + \alpha \\ s^{12}(\alpha^2) = 0,\ s^{12[1]}(\alpha^2) &= 0,\ s^{12[2]}(\alpha^2) = \alpha \end{aligned}$$

from which, by applying Corollary 4, we find

$$m_0 = 4, m_1 = 2, m_2 = 2.$$

It follows that the linear complexity of $\tilde{\mathbf{s}}$ is $\mathcal{L}(\tilde{\mathbf{s}}) = m_0 + m_1 + m_2 = 8$. Because, by Proposition 2, m_i is the multiplicity of α^i as a zero of the minimum degree connection polynomial $C(D)$, we can compute this polynomial as

$$C(D) = (1+D)^4(1+\alpha+D)^2(\alpha+D)^2 = (1+D)^4(1+D+D^2)^2$$

but we have no need to make this calculation if our interest is only in the linear complexity of $\tilde{\mathbf{s}}$.

We now introduce a matrix that we will find useful in connection with the generalized DFT in the next section.

Definition 5. The *Hasse matrix* $H_k(D)$ over a field F is the $k \times k$ matrix whose (i,j)-entry is $\binom{j-1}{i-1} D^{j-i}$, the $(i-1)^{\text{th}}$ Hasse derivative of the monomial D^{j-1} in $F[D]$.

Example 2. In a field F of characteristic 2,

$$H_4(D) = \begin{bmatrix} 1 & D & D^2 & D^3 \\ 0 & 1 & 0 & D^2 \\ 0 & 0 & 1 & D \\ 0 & 0 & 0 & 1 \end{bmatrix} .$$

Because a Hasse matrix is upper triangular with 1's on the main diagonal, it is invertible. The inverse matrix is easily obtained.

Lemma 6. *The inverse of the Hasse matrix $H_k(D)$ is $H_k(-D)$.*

Proof: The lemma follows immediately from the binomial expansion

$$(1-1)^j = \sum_{l \le k} \binom{j}{l} (-1)^l = 0$$

applied to the off-diagonal terms in the product $H_k(D)H_k(-D)$.

Remark. The lemma implies that in fields of characteristic 2, where $-1 = +1$, the matrix $H_k(D)$ is self-inverse.

4 A Generalized Discrete Fourier Transform (GDFT)

We first review the conventional discrete Fourier transform (DFT). Suppose now that $\mathbf{s}^N = [s_0, s_1, \cdots, s_{N-1}]$ is an arbitrary N-tuple with components in a field F and that there exists a primitive N^{th} root of unity, α, in F or some extension of F. Then, the Discrete Fourier Transform (DFT) of the "time- domain" N-tuple $\mathbf{s}^N$ is defined to be the "frequency-domain" N- tuple, $\mathbf{S}^N = [S_0, S_1, \cdots, S_{N-1}]$, given by

$$\mathbf{S}^N = [s^N(1), s^N(\alpha), \cdots, s^N(\alpha^{N-1})]$$

where as before

$$s^N(D) = s_0 + s_1 D + s_2 D^2 + \cdots + s_{N-1} D^{N-1}.$$

The time-domain N-tuple $\mathbf{s}^N$ can be recovered from its DFT $\mathbf{S}^N$ in the manner that

$$\mathbf{s}^N = \frac{1}{N}[S^N(1), S^N(\alpha^{-1}), \cdots, S^N(\alpha^{-(N-1)})]$$

where

$$S^N(X) = S_0 + S_1 X + S_2 X^2 + \cdots + S_{N-1} X^{N-1}.$$

Here, N denotes the element of the field F given by the sum of N 1's. In particular, if the field F has prime characteristic p, then N is taken modulo p. We will write

$$\mathbf{S}^N = \text{DFT}_\alpha(\mathbf{s}^N)$$

to emphasize the dependence of the DFT on the choice of the primitive N^{th} root of unity, α.

Again let $\tilde{\mathbf{s}}$ denote the *N-periodic* semi-infinite sequence

$$\tilde{\mathbf{s}} = s_0, s_1, \cdots, s_{N-1}, s_0, s_1, \cdots$$

obtained by endlessly repeating the N-tuple $\mathbf{s}^N$. [Note that the *period* of $\tilde{\mathbf{s}}$ may be a proper divisor of N.] The DFT possesses many properties that are useful in the analysis of such N-periodic sequences, cf. [11], in particular "Blahut's Theorem",

which asserts that the linear complexity of $\tilde{\mathbf{s}}$ is equal to the Hamming weight of $\mathrm{DFT}_\alpha(\mathbf{s}^N)$.

Of particular interest in cryptography is the case where F is the finite field $GF(q) = GF(p^r)$. The necessary and sufficient condition for $GF(q)$ to contain a primitive N-th root of unity is that N and p be relatively prime, i.e., that $\gcd(N,p) = 1$. The usual DFT is thus useful in the analysis of N-periodic q-ary sequences just when $\gcd(N,p) = 1$. Several authors, [2], [5], [12], have proposed generalizations of the DFT that permit its application to N-tuples with $\gcd(N,p) \neq 1$. One purpose of this paper is to propose a new such generalization of the DFT that was inspired by that in [5] but is somewhat simpler.

Let $\mathbf{s}^N = [s_0, s_1, \cdots, s_{N-1}]$ be an arbitrary N-tuple with components in a field F of prime characteristic p and suppose that $N = np^\nu$ where $\gcd(n,p) = 1$. Let α be a primitive n^{th} root of unity in F and let $s^{N[i]}(D)$ denote the i^{th} Hasse derivative of $s^N(D)$.

Definition 7. The *generalized discrete Fourier transform (GDFT)* of the N-tuple $\mathbf{s}^N = [s_0, s_1, \cdots, s_{N-1}]$, where $N = np^\nu$ and $\gcd(n,p) = 1$, is the $p^\nu \times n$ matrix $\mathbf{S}^{p^\nu \times n}$ given by

$$\mathbf{S}^{p^\nu \times n} = \mathrm{GDFT}_\alpha(\mathbf{s}^N) = \begin{bmatrix} s^N(1) & s^N(\alpha) & \cdots & s^N(\alpha^{n-1}) \\ s^{N[1]}(1) & s^{N[1]}(\alpha) & \cdots & s^{N[1]}(\alpha^{n-1}) \\ \vdots & & & \\ s^{N[p^\nu-1]}(1) & s^{N[p^\nu-1]}(\alpha) & \cdots & s^{N[p^\nu-1]}(\alpha^{n-1}) \end{bmatrix}.$$

When $\nu = 0$, the GDFT reduces to the usual DFT. We will soon see that the GDFT is indeed an invertible transformation, as is always demanded of a "transform."

Example 3. Continuing Example 1, we see that to compute $\mathrm{GDFT}_\alpha(\mathbf{s}^{12})$ according to its definition, we require the following additional evaluations of Hasse derivatives:

$$s^{12[1]}(1) = 0, s^{12[2]}(1) = 0, s^{12[3]}(1) = 0,$$
$$s^{12[3]}(\alpha) = 0$$
$$s^{12[3]}(\alpha^2) = 0.$$

This gives

$$\mathrm{GDFT}_\alpha(\mathbf{s}^{12}) = \mathbf{S}^{4\times 3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1+\alpha & \alpha \\ 0 & 0 & 0 \end{bmatrix}.$$

We now interpret Corollary 4 in terms of our GDFT. Toward this end, we make the following definition.

Definition 8. The *Günther weight* of a rectangular array is the number of its entries that are non-zero or that lie below a non-zero entry.

The multiplicity, m_i, of α^i as a zero of $C(D)$, as defined in Proposition 2, is specified in Corollary 4 in a manner that is seen to be just the number of entries that are non-zero or that lie below non- zero entries in the $(i+1)^{\text{st}}$ column of the GDFT $\mathbf{S}^{p^\nu \times n}$ of the N-tuple $\mathbf{s}^N$ obtained from the N-periodic sequence $\tilde{\mathbf{s}}$. The immediate consequence is the following very useful result.

Theorem 9 (Günther-Blahut Theorem). *The linear complexity of the F-ary N-periodic sequence $\tilde{\mathbf{s}} = s_0, s_1, \cdots, s_{N-1}, s_0, \cdots, s_{2N-1}, s_0, \cdots$, where F is a finite field of characteristic p and where $N = np^\nu$ with $\gcd(n,p) = 1$, is the Günther weight of the GDFT $\mathbf{S}^{p^\nu \times n}$ of the N-tuple $\mathbf{s}^N = [s_0, s_1, \cdots, s_{N-1}]$.*

When $\nu = 0$ so that $n = N$ and the GDFT array $\mathbf{S}^{p^\nu \times n}$ reduces to a one-row matrix, then the Günther weight of $\mathbf{S}^{p^\nu \times n}$ is just its Hamming weight. Thus this theorem is a natural generalization of Blahut's theorem for the usual DFT. We have called this generalization the "Günther-Blahut Theorem" [and the corresponding generalization of Hamming weight the "Günther weight"] because its content is equivalent to a result given by Günther in [5], who derived it from properties of the somewhat different generalization of the DFT that he introduced there.

Example 4. The GDFT array $\text{GDFT}_\alpha(\mathbf{s}^{12}) = \mathbf{S}^{4\times 3}$ of Example 3 is seen to have Günther weight 8, which shows that the 12- periodic sequence $\tilde{\mathbf{s}}$ has linear complexity 8, in agreement with the computation of Example 1.

More insight into the GDFT can be obtained by first writing $s^N(D)$ in the form

$$s^N(D) = s^n_{(0)}(D^{p^\nu}) + Ds^n_{(1)}(D^{p^\nu}) + \cdots + D^{(p^\nu-1)}s^n_{(p^\nu-1)}(D^{p^\nu})$$

where

$$s^n_{(i)}(D) = s_i + s_{i+p^\nu}D + \cdots + s_{i+(n-1)p^\nu}D^{n-1}$$

is the polynomial associated with the n-tuple $\mathbf{s}^n_{(i)} = [s_i, s_{i+p^\nu}, \cdots, s_{i+(n-1)p^\nu}]$ obtained by taking every $(p^\nu)^{\text{th}}$ digit of $\mathbf{s}^N$ starting with s_i, i.e., $\mathbf{s}^n_{(i)}$ is the i^{th} phase of the *decimation* of $\mathbf{s}^N$ by p^ν. Next, we define the "time-domain" array $\mathbf{s}^{p^\nu \times n}$ to be the $p^\nu \times n$ matrix

$$\mathbf{s}^{p^\nu \times n} = \begin{bmatrix} \mathbf{s}^n_{(0)} \\ \mathbf{s}^n_{(1)} \\ \vdots \\ \mathbf{s}^n_{(p^\nu-1)} \end{bmatrix} = \begin{bmatrix} s_0 & s_{p^\nu} & \cdots s_{(n-1)p^\nu} \\ s_1 & s_{1+p^\nu} & \cdots s_{1+(n-1)p^\nu} \\ \vdots & & \\ \vdots & & \\ s_{p^\nu-1} & s_{p^\nu-1+p^\nu} & \cdots s_{p^\nu-1+(n-1)p^\nu} \end{bmatrix}.$$

Now let β be another and possibly different n^{th} root of unity in F or some extension of F and define the matrix $\text{DFT}_\beta(\mathbf{s}^{p^\nu \times n})$ to be the $p^\nu \times n$ matrix

$$\text{DFT}_\beta(\mathbf{s}^{p^\nu \times n}) = \begin{bmatrix} \text{DFT}_\beta(\mathbf{s}^n_{(0)}) \\ \text{DFT}_\beta(\mathbf{s}^n_{(1)}) \\ \vdots \\ \text{DFT}_\beta(\mathbf{s}^n_{(p^\nu-1)}) \end{bmatrix}$$

whose $(i+1)^{\text{st}}$ row is the conventional DFT with respect to β of the n-tuple $\mathbf{s}^n_{(i)}$. Taking Hasse derivatives in the expression

$$s^N(D) = s^n_{(0)}(D^{p^\nu}) + Ds^n_{(1)}(D^{p^\nu}) + \cdots + D^{(p^\nu-1)}s^n_{(p^\nu-1)}(D^{p^\nu})$$

for $s^N(D)$ gives directly

$$\begin{bmatrix} s^N(D) \\ s^{N[1]}(D) \\ \vdots \\ s^{N[p^\nu-1]}(D) \end{bmatrix} = H_{p^\nu}(D) \begin{bmatrix} s^n_{(0)}(D^{p^\nu}) \\ s^n_{(1)}(D^{p^\nu}) \\ \vdots \\ s^n_{(p^\nu-1)}(D^{p^\nu}) \end{bmatrix}.$$

We now choose $\beta = \alpha^{p^\nu}$ and note that, because $\gcd(n, p^\nu) = 1$, β is indeed a primitive n^{th} root of unity. It follows that

$$\begin{bmatrix} s^N(\alpha^i) \\ s^{N[1]}(\alpha^i) \\ \vdots \\ s^{N[p^\nu-1]}(\alpha^i) \end{bmatrix} = H_{p^\nu}(\alpha^i) \begin{bmatrix} s^n_{(0)}(\beta^i) \\ s^n_{(1)}(\beta^i) \\ \vdots \\ s^n_{(p^\nu-1)}(\beta^i) \end{bmatrix}. \tag{4}$$

The vector on the left in this equation is just the $(i+1)^{\text{st}}$ column of the matrix $\mathbf{S}^{p^\nu \times n} = \text{GDFT}_\alpha(\mathbf{s}^N)$, while the vector on the right is just the $(i+1)^{\text{st}}$ column of the matrix $\text{DFT}_\beta(\mathbf{s}^{p^\nu \times n})$. Because the matrix $H_{p^\nu}(\alpha^i)$ is invertible, it follows that one can recover $\text{DFT}_\beta(\mathbf{s}^{p^\nu \times n})$ from $\text{GDFT}_\alpha(\mathbf{s}^N)$ and of course one can then recover $\mathbf{s}^{p^\nu \times n}$, and hence also $\mathbf{s}^N$ from $\text{DFT}_\beta(\mathbf{s}^{p^\nu \times n})$. It follows that the GDFT is indeed invertible.

Example 5. Continuing with 3, we have the $p^\nu \times n = 4 \times 3$ time- domain array

$$\mathbf{s}^{4\times 3} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Noting that $\beta = \alpha^{p^\nu} = \alpha^4 = \alpha$, we obtain

$$\text{DFT}_\beta(\mathbf{s}^{4\times 3}) = \text{DFT}_\alpha(\mathbf{s}^{4\times 3}) = \begin{bmatrix} \text{DFT}_\alpha([0,1,0]) \\ \text{DFT}_\alpha([0,0,0]) \\ \text{DFT}_\alpha([1,1,0]) \\ \text{DFT}_\alpha([0,0,0]) \end{bmatrix} = \begin{bmatrix} 1 & \alpha & 1+\alpha \\ 0 & 0 & 0 \\ 0 & 1+\alpha & \alpha \\ 0 & 0 & 0 \end{bmatrix}.$$

Pre-multiplying each column of $\text{DFT}_\beta(\mathbf{s}^{4\times 3})$ by the corresponding one of the following matrices:

$$H_4(1) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, H_4(\alpha) = \begin{bmatrix} 1 & \alpha & 1+\alpha & 1 \\ 0 & 1 & 0 & 1+\alpha \\ 0 & 0 & 1 & \alpha \\ 0 & 0 & 0 & 1 \end{bmatrix}, H_4(\alpha^2) = \begin{bmatrix} 1 & 1+\alpha & \alpha & 1 \\ 0 & 1 & 0 & \alpha \\ 0 & 0 & 1 & 1+\alpha \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

gives again the matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1+\alpha & \alpha \\ 0 & 0 & 0 \end{bmatrix} = \mathbf{S}^{4\times 3} = \mathrm{GDFT}_{\alpha}(\mathbf{s}^{12})$$

in agreement with the computation in Example 3.

5 Applications of the Generalized DFT

5.1 The Games-Chan Algorithm and its generalization

The theory of the GDFT presented in the previous section specializes in an interesting way to the case we now consider where the components of the N-periodic sequence $\tilde{\mathbf{s}}$ lie in a finite field of characteristic 2 and $N = 2^{\nu}$ so that $n = 1$. The time-domain array $\mathbf{s}^{2^{\nu}\times 1}$ is now just the transpose of the 2^{ν}-tuple $\mathbf{s}^{2^{\nu}} = [s_0, s_1, \cdots, s_{2^{\nu}-1}]$. Because $\alpha = 1$ is the only first root of unity, the DFT for length $n = 1$ is just the identity transformation so that $\mathrm{DFT}_1(\mathbf{s}^{2^{\nu}\times 1}) = (\mathbf{s}^{2^{\nu}})^{\mathrm{T}}$ where, here and hereafter, the superscript $^{\mathrm{T}}$ denotes transposition. The GDFT also reduces to a single column that, according to (4), is given by

$$\mathrm{GDFT}_1(\mathbf{s}^{2^{\nu}}) = \mathrm{H}_{2^{\nu}}(1)(\mathbf{s}^{2^{\nu}})^{\mathrm{T}}. \tag{5}$$

The matrix $H_{2^{\nu}}(1)$ has an especially simple form.

Lemma 10. *In any field of characteristic 2 and for any integer $\nu \geq 1$,*

$$H_{2^{\nu}}(1) = \begin{bmatrix} H_{2^{\nu-1}}(1) & H_{2^{\nu-1}}(1) \\ 0 & H_{2^{\nu-1}}(1) \end{bmatrix}. \tag{6}$$

Proof. By the definition of the Hasse matrix, the entry in row $i+1$ and column $j+1$ of $H_{2^{\nu}}(1)$ is $\binom{j}{i}$. To prove the lemma then, it suffices to show that

$$\binom{j}{i} = \binom{2^{\nu-1}+j}{i} = \binom{2^{\nu-1}+j}{2^{\nu-1}+i}$$

for $0 \leq i < 2^{\nu-1}$ and $0 \leq j < 2^{\nu-1}$. But, by a theorem of Lucas [10] (cf. also [1], p. 113), for any prime p, any positive integer ν, and any integers i and j satisfying $0 \leq i < p^{\nu}$ and $0 \leq j < p^{\nu}$,

$$\binom{j}{i} \equiv \prod_{k=0}^{\nu-1} \binom{j_k}{i_k} \qquad (\mathrm{mod}\quad \mathrm{p}) \tag{7}$$

where $[j_{\nu-1}, \cdots, j_1, j_0]_p$ and $[i_{\nu-1}, \cdots, i_1, i_0]_p$ are the radix-p representations of i and j, respectively. For $p = 2$ and for $0 \leq i < 2^{\nu-1}$ and $0 \leq j < 2^{\nu-1}$, the radix-2 representations of j and $2^{\nu-1}+j$ are $[0, j_{\nu-2}, \cdots, j_1, j_0]_2$ and $[1, j_{\nu-2}, \cdots, j_1, j_0]_2$, respectively. Similarly, the radix-2 representations of i and $2^{\nu-1}+i$ are $[0, i_{\nu-2}, \cdots, i_1, i_0]_2$ and $[1, i_{\nu-2}, \cdots, i_1, i_0]_2$, respectively. The equalities claimed in the lemma now follow immediately from (7) and the fact that $\binom{0}{0} = \binom{1}{0} = \binom{1}{1} = 1$

We now split the time-domain sequence into its left and right halves in the manner $\mathbf{s}^{2^\nu} = [\mathbf{s}_L^{2^{\nu-1}} : \mathbf{s}_R^{2^{\nu-1}}]$ where $\mathbf{s}_L^{2^{\nu-1}} = [s_0, s_1, \cdots, s_{2^{\nu-1}-1}]$ and $\mathbf{s}_R^{2^{\nu-1}} = [s_{2^{\nu-1}}, s_{2^{\nu-1}+1}, \cdots, s_{2^\nu-1}]$. We can then write

$$\mathrm{GDFT}(\mathbf{s}^{2^\nu}) = \begin{bmatrix} H_{2^{\nu-1}}(1) & H_{2^{\nu-1}}(1) \\ 0 & H_{2^{\nu-1}}(1) \end{bmatrix} \begin{bmatrix} (\mathbf{s}_L^{2^{\nu-1}})^T \\ (\mathbf{s}_R^{2^{\nu-1}})^T \end{bmatrix}$$

and hence

$$\mathrm{GDFT}(\mathbf{s}^{2^\nu}) = \begin{bmatrix} H_{2^{\nu-1}}(1)(\mathbf{s}_L^{2^{\nu-1}} + \mathbf{s}_R^{2^{\nu-1}})^T \\ H_{2^{\nu-1}}(1)(\mathbf{s}_R^{2^{\nu-1}})^T \end{bmatrix}. \tag{8}$$

Because the Hasse matrix $H_{2^{\nu-1}}(1)$ is non-singular, it now follows from the Günther-Blahut Theorem that: 1) if $\mathbf{s}_L^{2^{\nu-1}} + \mathbf{s}_R^{2^{\nu-1}} = \mathbf{0}$, then the linear complexity of the 2^ν- periodic sequence $\mathcal{L}(\tilde{\mathbf{s}})$ of $\tilde{\mathbf{s}}$ is the same as that of the $2^{\nu-1}$-periodic sequence having $\mathbf{s}_R^{2^{\nu-1}}$ as its first $2^{\nu-1}$ digits; but 2) if $\mathbf{s}_L^{2^{\nu-1}} + \mathbf{s}_R^{2^{\nu-1}} \neq \mathbf{0}$, then $\mathcal{L}(\tilde{\mathbf{s}})$ is $2^{\nu-1}$ plus the linear complexity of the $2^{\nu-1}$-periodic sequence having $\mathbf{s}_L^{2^{\nu-1}} + \mathbf{s}_R^{2^{\nu-1}}$ as its first $2^{\nu-1}$ digits. These considerations immediately establish the validity of the following simple algorithm for determining the linear complexity of the 2^ν-periodic sequence $\tilde{\mathbf{s}}$.

Algorithm 1 (Games-Chan) *Enter ν and the first 2^ν digits $\mathbf{s}^{2^\nu}$ of the 2^ν-periodic sequence $\tilde{\mathbf{s}}$ with components in a finite field of characteristic 2.*
Set $L := 0$
REPEAT
  Split the sequence $\mathbf{s}^{2^\nu}$ into its left and right halves $\mathbf{s}_L^{2^{\nu-1}}$ and $\mathbf{s}_R^{2^{\nu-1}}$, respectively.
  IF $\mathbf{s}_L^{2^{\nu-1}} + \mathbf{s}_R^{2^{\nu-1}} = \mathbf{0}$ *THEN replace* $\mathbf{s}^{2^\nu}$ *by* $\mathbf{s}_R^{2^{\nu-1}}$
  ELSE set $L := L + 2^{\nu-1}$ *and replace* $\mathbf{s}^{2^\nu}$ *by* $\mathbf{s}_L^{2^{\nu-1}} + \mathbf{s}_R^{2^{\nu-1}}$.
  Decrement ν by 1.
UNTIL $\nu = 0$.
IF $\mathbf{s}^1 \neq 0$ *THEN set* $L := L + 1$.
Output L, the linear complexity $\mathcal{L}(\tilde{\mathbf{s}})$ of $\tilde{\mathbf{s}}$.

This algorithm is precisely the well-known Games-Chan algorithm [4], cf. also [14], which was originally formulated for binary sequences. The argument from the GDFT given here shows that the algorithm can be used unchanged for sequences over any finite field of characteristic 2.

It is now also an easy matter to generalize the Games-Chan algorithm to p^ν-periodic sequences with digits in a finite field of characteristic p, as we now explain for the case $p = 3$. For this case, the recursion (6) becomes

$$H_{p^\nu}(1) = \begin{bmatrix} H_{p^{\nu-1}}(1) & H_{p^{\nu-1}}(1) & H_{p^{\nu-1}}(1) \\ 0 & H_{p^{\nu-1}}(1) & 2H_{p^{\nu-1}}(1) \\ 0 & 0 & H_{p^{\nu-1}}(1) \end{bmatrix}.$$

It follows that when the first 3^ν digits $\mathbf{s}^{3^\nu}$ of the 3^ν- periodic sequence $\tilde{\mathbf{s}}$ are split into their left, middle and right thirds $\mathbf{s}_L^{3^{\nu-1}}$, $\mathbf{s}_M^{3^{\nu-1}}$ and $\mathbf{s}_R^{3^{\nu-1}}$, respectively, then

in place of (8) one obtains

$$\mathrm{GDFT}(\mathbf{s}^{3^\nu}) = \begin{bmatrix} H_{3^{\nu-1}}(1)(\mathbf{s}_L^{3^{\nu-1}} + \mathbf{s}_M^{3^{\nu-1}} + \mathbf{s}_R^{3^{\nu-1}})^T \\ H_{3^{\nu-1}}(1)(\mathbf{s}_M^{3^{\nu-1}} + 2\mathbf{s}_R^{3^{\nu-1}})^T \\ H_{3^{\nu-1}}(1)(\mathbf{s}_R^{3^{\nu-1}})^T \end{bmatrix}.$$

Because the Hasse matrix $H_{3^{\nu-1}}(1)$ is non-singular, it now follows from the Günther-Blahut Theorem that: 1) if $\mathbf{s}_L^{3^{\nu-1}} + \mathbf{s}_M^{3^{\nu-1}} + \mathbf{s}_R^{3^{\nu-1}} = \mathbf{0}$ and $\mathbf{s}_M^{3^{\nu-1}} + 2\mathbf{s}_R^{3^{\nu-1}} = \mathbf{0}$, then the linear complexity $\mathcal{L}(\tilde{\mathbf{s}})$ of the 3^ν-periodic sequence $\tilde{\mathbf{s}}$ is the same as that of the $3^{\nu-1}$-periodic sequence having $\mathbf{s}_R^{3^{\nu-1}}$ as its initial segment; 2) if $\mathbf{s}_L^{3^{\nu-1}} + \mathbf{s}_M^{3^{\nu-1}} + \mathbf{s}_R^{3^{\nu-1}} = \mathbf{0}$ but $\mathbf{s}_M^{3^{\nu-1}} + 2\mathbf{s}_R^{3^{\nu-1}} \neq \mathbf{0}$, then $\mathcal{L}(\tilde{\mathbf{s}})$ is $3^{\nu-1}$ plus the linear complexity of the $3^{\nu-1}$-periodic sequence having $\mathbf{s}_L^{3^{\nu-1}} + 2\mathbf{s}_R^{3^{\nu-1}}$ as its initial segment; and finally 3) if $\mathbf{s}_L^{3^{\nu-1}} + \mathbf{s}_M^{3^{\nu-1}} + \mathbf{s}_R^{3^{\nu-1}} \neq \mathbf{0}$ then $\mathcal{L}(\tilde{\mathbf{s}})$ is $2 \times 3^{\nu-1}$ plus the linear complexity of the $3^{\nu-1}$-periodic sequence having $\mathbf{s}_L^{3^{\nu-1}} + \mathbf{s}_M^{3^{\nu-1}} + \mathbf{s}_R^{3^{\nu-1}}$ as its initial segment. The necessary modification of the Games-Chan algorithm is now obvious and its description will be omitted. For an arbitrary prime p, the analogous argument shows that $\mathbf{s}^{p^\nu}$ can be split into p disjoint subsequences of length $p^{\nu-1}$ and the linear complexity of the p^ν-periodic sequence $\tilde{\mathbf{s}}$ determined from p linear combinations of these sequences. Again we omit the obvious details.

5.2 Application to Hadamard products of sequences

We now show the utility of the GDFT for the analysis of sequences obtained by memoryless nonlinear combining of periodic sequences, an operation often performed in the running-key generators of additive stream ciphers. Such operations can always be expressed as a linear combination of various Hadamard products of the input sequences, where by a *Hadamard product* is meant a componentwise multiplication of the sequences, which we denote by $\wedge$.

Let $\tilde{\mathbf{t}}$ and $\tilde{\mathbf{u}}$ be q-ary N-periodic sequences where $q = p^\nu$, $\mathrm{N} = np^\nu$ and $\gcd(n, p) = 1$ and let $\tilde{\mathbf{s}}$ be the Hadamard product $\tilde{\mathbf{t}} \wedge \tilde{\mathbf{u}}$. Then $\mathbf{s}^N$ is also the Hadamard product $\mathbf{t}^N \wedge \mathbf{u}^N$ of $\mathbf{t}^N$ and $\mathbf{u}^N$. But it is also true for subsequences that

$$\mathbf{s}_{(i)}^n = [s_i, s_{i+p^\nu}, \cdots, s_{i+(n-1)p^\nu}] = \mathbf{t}_{(i)}^n \wedge \mathbf{u}_{(i)}^n$$

where $\mathbf{t}_{(i)}^n = [t_i, t_{i+p^\nu}, \cdots, t_{i+(n-1)p^\nu}]$ and $\mathbf{u}_{(i)}^n = [u_i, u_{i+p^\nu}, \cdots, u_{i+(n-1)p^\nu}]$. By the convolution property of the (usual) DFT_β for length n, cf. [11], the DFT $\mathbf{S}_{(i)}^n$ of $\mathbf{s}_{(i)}^n$ is $\frac{1}{n}$ times the circular convolution $\mathbf{U}_{(i)}^n \otimes \mathbf{T}_{(i)}^n$ of the length-n DFT_β's $\mathbf{T}_{(i)}^n$ and $\mathbf{U}_{(i)}^n$ of $\mathbf{t}_{(i)}^n$ and $\mathbf{u}_{(i)}^n$, *respectively*. Hence, we have

$$\mathrm{DFT}_\beta(\mathbf{s}^{\mathrm{p}^\nu \times \mathrm{n}}) = \frac{1}{\mathrm{n}} \mathbf{T} \otimes \mathbf{U} \tag{9}$$

where we have introducted the notation for arrays

$$\mathbf{T} \otimes \mathbf{U} = \begin{bmatrix} \mathbf{U}_{(0)}^n \otimes \mathbf{T}_{(0)}^n \\ \mathbf{U}_{(1)}^n \otimes \mathbf{T}_{(1)}^n \\ \vdots \\ \mathbf{U}_{(p^\nu-1)}^n \otimes \mathbf{T}_{(p^\nu-1)}^n \end{bmatrix}.$$

This formulation, together with (4), implies that the theory of linear complexity for Hadamard products of N-periodic sequences for general N can be obtained directly from the theory for the well-studied special case where $\gcd(N,p) = 1$.

6 Acknowledgement

The authors are grateful to Prof. Xuduan Lin, currently visiting at the ETH Zürich, for his careful reading of, and very helpful comments on, an earlier version of this paper, to Dr. Kaisa Nyberg of Helsinki for directing their attention to [6], and to the anonymous referees for their constructive suggestions.

References

1. E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
2. S. R. Blackburn, "A Generalisation of the Discrete Fourier Transform: Determining the Minimal Polynomial of a Periodic Sequence," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1702-1704, Nov. 1994.
3. G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. Seemann, "On Repeated-Root Cyclic Codes", *IEEE Trans. Inform. Theory*, vol. IT-37, pp. 337-342, March 1991.
4. R. A. Games and A. H. Chan, "A Fast Algorithm for Determining the Complexity of a Binary Sequence with Period 2^n," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 144-146, Jan. 1983.
5. C. G. Günther, "A Finite Field Fourier Transform for Vectors of Arbitrary Length," pp. 141-153 in *Communications and Cryptography: Two Sides of One Tapestry* (Eds. R. E. Blahut, D. J. Costello, Jr., U. Maurer and T. Mittelholzer). Norwell, MA, and Dordrecht, NL: Kluver Academic, 1994.
6. R. Göttfert and H. Niederreiter, "Hasse-Teichmüller Derivatives and Products of Linear Recurring Sequences," *Comtemporary Mathematics*, vol. 168, pp.117-125, 1994.
7. H. Hasse, "Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenen Konstantenkörper bei beliebiger Charakteristik," *J. Reine u. Ang. Math.*, vol. 175, pp. 50-54, 1936.
8. E. L. Key, "An analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators," *IEEE Trans. Inform. Th.*, vol. IT-22, pp. 732- 736, Nov. 1976.
9. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20. Englewood Cliffs, NJ: Addison-Wesley, 1983.
10. M. E. Lucas, "Sur les congruences des nombres euleriennes et des coefficients diffénticls des functions trigonométriques, suivant un-module premier," *Bull. Soc. Math. France*, vol. 6, pp. 49-54, 1878.
11. J. L. Massey and S. Serconek, "A Fourier Transform Approach to the Linear Complexity of Nonlinearly Filtered Sequences," *Advances in Cryptology-CRYPTO '94* (Ed. Y. G. Desmedt), Lecture Notes in Computer Science No. 839. New York: Springer, pp.322-340, 1994.
12. P. Mathys, "A Generalization of the Discrete Fourier Transform in Finite Fields," *Proc. IEEE Symp. Inform. Theory*, San Diego (CA), pp. 14-19, 1990.
13. K. Paterson, "On the Linear Complexity of Nonlinearly Filtered m-sequences," preliminary manuscript, Feb. 2, 1996.

14. M. Robshaw, "On Evaluating the Linear Complexity of a Sequence of Least Period 2^n," *Designs, Codes and Cryptography*, vol. 4, pp. 263-269, 1994.
15. R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Heidelberg and New York: Springer, 1986.
16. O. Teichmüller, "Differentialrechnung bei Charackteristik p," *J. Reine u. Ang. Math.*, vol. 175, pp. 89-99, 1936.

This article was processed using the LaTeX macro package with LLNCS style