(Reprinted from Proceedings, Second Joint Swedish-Soviet International Workshop on Information Theory, Gränna, Sweden, April 14-19, 1985)

DELAYED-DECIMATION/SQUARE SEQUENCES

J. L. Massey
Institute for Signal and Information Processing
Swiss Federal Institute of Technology
CH-8092 ZURICH, SWITZERLAND

Abstract: A delayed-decimation/square (DDS) sequence is defined as a semi-infinite sequence of digits in a field of characteristic 2 whose square coincides with its (second) decimation begun with the second digit. The conditions for a sequence to be DDS are derived; and examples of the appearance of DDS sequences in coding and cryptography are given.

Introduction.

The aim of this paper is to identify a structural property of sequences that has relevance in both error-correction coding and cryptography.

We shall consider only semi-infinte sequences $\underset{\sim}{s}=(s_0,s_1,s_2,..)$ whose components are in a field of characteristic 2. Such a sequence will be said to be a decimation/square (DS) sequence if its second decimation $(s_0,s_2,s_4,...)$ coincides with the sequence of squared components $(s_0^2,s_1^2,s_2^2,...)$, or, equivalently, if $s_{2i} = s_i^2$ for all $i \geq 0$. It is somewhat arbitrary whether one begins the decimated sequence with s_0 or s_1. Thus, we shall say that s is a delayed-decimation/square (DDS) sequence if $(s_1,s_3,s_5,...)$ coincides with $(s_0^2,s_1^2,s_2^2,...)$, i.e., if

$$s_i^2 = s_{2i+1}, \quad \text{all } i \geq 0. \tag{1}$$

In the special case of a binary sequence, $s_i^2 = s_i$ so that the sequence of squared components is just $\underset{\sim}{s}$ itself.

The thesis of this paper is that the DDS property is actually more natural (and useful) than the apparently more natural DS property.

Characterization of DDS Sequences.

It is useful to characterize the sequence $\underset{\sim}{s} = (s_0,s_1,s_2,...)$ by its D-transform

$$S(D) = s_0 + s_1D + s_2D^2 + \ldots . \tag{2}$$

Taking formal derivatives in (2) gives

$$S'(D) = s_1 + s_3D^2 + s_5D^4 + \ldots . \tag{3}$$

Squaring in (2) gives

$$S^2(D) = s_0^2 + s_1^2D^2 + s_2^2D^4 + \ldots . \tag{4}$$

Comparison of (3) and (4) with (1) gives immediately the following simple characterization of a DDS sequence.

Proposition 1: The sequence $\underset{\sim}{s}$ is a DDS sequence if and only if $S^2(D) = S'(D)$.

By way of comparison, we remark that the condition for $\underset{\sim}{s}$ to be DS is the rather more awkward one that $S^2(D) = S(D) + DS'(D)$.

Our greatest interest will be in periodic sequences, i.e., sequences $\underset{\sim}{s} = (s_0,s_1,s_2,...)$ such that, for some positive integer N, $s_i = s_{i+N}$ for all $i \geq 0$. (The smallest such N is the fundamental period of the sequence.) As is well-known, the D-transform of a periodic sequence $\underset{\sim}{s}$ can be written as

$$S(D) = P(D)/C(D), \tag{5}$$

where $C(D) = 1 + c_1D + \ldots + c_LD^L$, $c_L \neq 0$, and

$$\deg [P(D)] < L = \deg [C(D)]. \tag{6}$$

The polynomial $C(D)$ is the connection polynomial of a linear feedback shift-register (LFSR) of length L that generates $\underset{\sim}{s}$ when its initial state is $[s_0,s_1,\ldots,s_{L-1}]$. When also

$$\gcd[P(D),C(D)] = 1, \tag{7}$$

then this is the unique shortest LFSR that can generate the sequence $\underset{\sim}{s}$ [1]. In this case, the fundamental period of $\underset{\sim}{s}$ is the smallest positive integer N such that $C(D)$ divides $1 - D^N$; this N is also sometimes called the <u>period</u> of $C(D)$.

<u>Proposition 2</u>: A periodic sequence $\underset{\sim}{s}$ is a DDS sequence if and only if its D-transform (5), satisfying (6) and (7), also satisfies $P(D) = C'(D)$.

<u>Proof</u>: Taking formal derivatives in (5) gives

$$S'(D) = [C(D)P'(D) + C'(D)P(D)]/C^2(D).$$

Thus, $\underset{\sim}{s}$ is DDI according to Proposition 1 if and only if

$$C(D)P'(D) + C'(D)P(D) = P^2(D). \tag{8}$$

It follows from (7) and (8) that if $\underset{\sim}{s}$ is DDS, then $P(D)$ divides $P'(D)$, which is possible if and only if $P'(D) = 0$. But $P'(D)=0$ gives, from (8), $P(D) = C'(D)$. Conversely, if $P(D) = C'(D)$, then $P'(D) = C''(D) = 0$; thus, (8) is satisfied and $\underset{\sim}{s}$ is DDS, as was to be shown.

<u>Some Examples of DDS Sequences</u>.

The syndrome sequence $\underset{\sim}{s} = (S_1,S_2,S_3,\ldots)$ of a primitive binary BCH code is a periodic sequence of elements from the field $GF(2^L)$, where $N = 2^L-1$ is the code length, satisfying $S_j^2 = S_{2j}$ for all $j \geq 1$. Thus, the fact that $s_i = S_{i+1}$ implies that $s_i^2 = S_{2i+2} = s_{2i+1}$, and hence that $\underset{\sim}{s}$ is a DDS sequence.

The <u>linear complexity</u> of a finite or semi-infinite sequence is the length of the shortest LFSR that generates the sequence. We write $L_n(\underset{\sim}{s})$ to denote the linear complexity of the finite

sequence $[s_0,s_1,s_2,\ldots,s_{n-1}]$. Rueppel [2] has recently conjectured that the binary sequence $\underset{\sim}{s}$ defined by

$$s_i = \begin{cases} 1, \text{ if } i+1 \text{ is a power of 2} \\ 0, \text{ otherwise} \end{cases} \tag{9}$$

satisfies

$$L_n(\underset{\sim}{s}) = \lfloor (n+1)/2 \rfloor, \quad \text{all } n \geq 0; \tag{10}$$

and has verified that (10) holds for $n \leq 127$. Now if $i + 1 = 2^j$, then $(2i + 1) + 1 = 2^{j+1}$. Thus (9) implies that $\underset{\sim}{s}$ satifies (1) and hence is a DDS sequence. This particular non-periodic sequence $\underset{\sim}{s} = (1,1,0,1,0,0,0,1,0,0,0,0,0,0,0,1,\ldots)$ would be of considerable interest in cryptography should the conjecture (10) be true, since the "linear complexity profile" given by (10) virtually coincides with the high probability linear complexity profile of a truly random binary sequence [2].

<u>Natural Phases and Idempotent Codewords</u>.

Suppose α is a primitive element of $GF(2^L)$ whose minimum polynomial is $h(X) = X^L + c_1X^{L-1} + \ldots + c_L$. Then the sequence $\underset{\sim}{s} = (s_0,s_1,s_2,\ldots)$ defined by

$$s_i = T_L(\alpha^i), \quad i \geq 0 \tag{11}$$

where T_L is the trace operator from $GF(2^L)$ to $GF(2)$, is called the <u>natural phase</u> of the pseudo-noise (PN) sequence generated by the length L LFSR with connection polynomial $C(D) = 1 + c_1D + \ldots + c_LD^L$. It follows from (11) that

$$s_{2i} = T_L(\alpha^{2i}) = T_L(\alpha^i) = s_i$$

and hence that the binary sequence $\underset{\sim}{s}$ is a DS sequence, not a DDS sequence. It is often desirable to compute the initial state $[s_0,s_1,\ldots,s_{L-1}]$ directly from $C(D)$, in order conveniently to generate $\underset{\sim}{s}$.

Let $\underset{\sim}{s}^* = (s_0^*,s_1^*,s_2^*,\ldots)$ be a DDS binary sequence. Then $\underset{\sim}{s} = (b,s_0^*,s_1^*,\ldots)$ is a DS binary sequence for both $b = 0$ and

$b = 1$. Conversely, if $\underset{\sim}{s} = (s_0, s_1, s_2, \ldots)$ is a DS sequence, then $\underset{\sim}{s}^* = (s_1, s_2, s_3, \ldots)$ is a DDS sequence.

It follows from Proposition 2 that the length L LFSR with connection polynomial C(D) generates a unique non-null DDS sequence $\underset{\sim}{s}^*$, where

$$S^*(D) = C'(D)/C(D). \tag{12}$$

Hence, the sequence $(b, s_0^*, s_1^*, \ldots)$ has the D-transform

$$b + D\,S^*(D) = [bC(D) + DC'(D)]/C(D).$$

The polynomial

$$P(D) = bC(D) + DC'(D) \tag{13}$$

satisfies (7) regardless of whether $b = 0$ or $b = 1$, because C(D) is irreducible; however, P(D) satisfies (6) if and only if b in (13) is chosen as

$$b = \begin{cases} 0, & \text{if } L = \deg[C(D)] \text{ is even} \\ 1, & \text{if } L \text{ is odd.} \end{cases} \tag{14}$$

With the choice (14), it follows that $(b, s_0^*, s_1^*, \ldots) = \underset{\sim}{s}$.

Example: For $L = 4$ and $C(D) = 1 + D^3 + D^4$, we have $C'(D) = D^2$. Thus

$$\begin{aligned} S^*(D) &= D^2/(1 + D^3 + D^4) \\ &= D^2 + D^5 + (\text{higher order terms}). \end{aligned}$$

It follows from (14) that $b = 0$. Hence

$$\begin{aligned} [s_0, s_1, s_2, s_3] &= [b, s_0^*, s_1^*, s_2^*] \\ &= [0,0,0,1] \end{aligned}$$

is the initial shift-register state for generation of the natural phase of the PN sequence.

In our opinion, the DDS sequence $\underset{\sim}{s}^*$ has a better claim to the title "natural" phase of the PN sequence than does the DS sequence $\underset{\sim}{s}$. Note that the components of $\underset{\sim}{s}^*$ satisfy

$$s_i^* = T_L(\alpha^{i+1}). \tag{15}$$

The slight additional complexity of (15) over (11) should be

compared with the simplicity of $P^*(D) = C'(D)$ as opposed to (13) and (14).

In fact, we can use (12) to define the "characteristic sequence" $\underset{\sim}{s}^*$ from any LFSR of length L whose connection polynomial C(D) has degree L and $C'(D) \neq 0$. [The condition $C'(D) = 0$ in a field of characteristic 2 in just the condition that C(D) is the square of another polynomial.] We could also define a "natural phase" $\underset{\sim}{s} = (b, s_0^*, s_1^*, \ldots)$ by choosing b in (13) so that (6) is satisfied. Defining $h(X) = X^L + c_1 X^{L-1} + \ldots + c_L$ as before and letting N be the period of C(D), we would find that $[s_0, s_1, \ldots, s_{N-1}]$ so obtained is just the generating idempotent codeword of the cyclic code with parity-check polynomial h(X). This may give the reader some insight into the assertion to be proved in the "hard" problem (17) of [3, p.223].

References.

[1] J.L. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Trans.Info.Th., vol. IT-15, pp.122-127, Jan. 1969.

[2] R.A. Rueppel, "New Approaches to Stream Ciphers", Ph.D. Dissertation, Swiss Federal Institute of Technology, Zurich, Dec. 1984.

[3] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes". Amsterdam: North-Holland, 1977.