Cross-Recurrence Property of m-Sequences

Farhad Hemmati
hemmatifarhad@yahoo.com

Abstract— **A binary maximal length sequence (m-sequence) of period L = 2^m - 1 can be generated by a binary m-stage linear feedback shift-register (LFSR). Tap connections of the LFSR corresponds to a binary primitive polynomial of degree m. m-sequences enjoy several well-known and unique properties. A new property for m-sequences, called cross-recurrence property, is presented in this paper and its potential applications are briefly outlined.**

Keywords: m-sequence, linear feedback shift-register, finite fields, polynomials over GF(2), cross-recurrence.

I. Introduction

Pseudo-Noise (PN) sequences, also known as maximal length sequences (or m-sequences) have several applications in communications, spread spectrum, radar, and cryptography; to name a few. A binary m-sequence of period L = 2^m - 1 can be generated by a binary m-stage linear feedback shift-register (LFSR). Tap connection (characteristic polynomial) of the LFSR corresponds to a binary primitive polynomial of degree m, [1]. m-sequences enjoy several well-known and unique properties. A new property for m-sequences, called cross-recurrence property, is presented and proved in the following. As potential applications of the new property, generation of non-linear maximal length feedback shift-register sequences and the discrete logarithm problem over finite fields are briefly outlined. Detail formulation of the algorithms and their complexity analysis is subject of forthcoming papers.

Section II includes definitions and notations. Main theorems are stated and proved in sections III and IV. Potential applications of the cross-recurrence property are briefly mentioned in section V. Polynomial addition and multiplication are carried out over the finite field of two elements, GF(2), [3].

II. Definitions and Notations

<u>State</u>: An m-dimensional binary vector, $S_i = (s_i, s_{i+1}, \ldots, s_{i+m-2}, s_{i+m-1})$[1], s_i = 0 or 1 for all i, $0 \le i \le L-1$, representing m consecutive bits over an m-sequence of period L = 2^m-1.

<u>Extended state of order d</u>: An m + d = k-dimensional binary vector, $E_i = (s_i, s_{i+1}, \ldots, s_{i+k-2,} s_{i+k-1})$[1], $0 \le i \le L-1$, representing k consecutive bits over an m-sequence of period L where d, $0 \le d < m$, is an integer.

<u>Unit vector</u>: A k-dimensional binary vector consisting of k-1 zeros followed by a single 1, U = (0, 0, 0, …, 0, 0, 1).

<u>Companion state</u>: Term by term modulo-2 addition of E_i and U; $C_i = E_i + U = (s_i, s_{i+1}, \ldots, s_{i+k-2,\ 1+} s_{i+k-1})$. In other words,

$$U = C_i + E_i \qquad (1)$$

i.e., term by term modulo-2 sum of a state and its companion is the unit vector.

<u>Degree (delay) of a polynomial</u>: The maximum (minimum) exponent of terms in a polynomial. Only polynomials of zero delay are considered in this paper.

<u>Characteristic state for a given binary polynomial f(x) of degree d < m</u>: An extended state of order d on an m-sequence whose companion satisfies the recurrence relation of f(x).

Clearly, any block of m + i, 0 > i > d, consecutive bits on the characteristic state not only satisfies the recurrence relation of g(x) but also the recurrence relation of f(x) hence, the <u>cross-recurrence property</u>.

<u>Example 1</u>: It is well known that every m-sequence of period L = 2^m -1 includes a block of m consecutive ones followed by a zero, E = (1, 1, …, 1, 1, 0). The companion of E; C = E + U = (1, 1, …, 1, 1, 1) consists of m+1 consecutive ones and satisfies the recurrence relation of f(x) = 1 + x. In other words, E + U can be generated by a one-stage LFSR with characteristic polynomial 1+x and initial state (1). Hence, E = (1, 1, …, 1, 1, 0) is the characteristic state on any m-sequence for the polynomial f(x) = 1+x.

Theorem 1, presented in the following section, is a generalization of example 1.

III. The Cross-recurrence Property of m-Sequences

<u>Theorem 1</u>: Let f(x) be a binary polynomial of degree d, 0 < d < m and zero delay. Then, a unique characteristic state of order d exists on an m-sequence generated by a primitive polynomial g(x), deg[g(x)] = m, such that its companion satisfies the recurrence relation of f(x).

[1] When exceeding L, subscripts are reduced modulo L.

Proof: In polynomial form, powers of an element x in GF(2^m), generated by g(x), can be written as, [3]:

$$x^j = f_j(x) \quad \text{mod}[g(x)], \quad \deg[f_j(x)] = d < m$$

or

$$x^j = f_j(x) + a(x)g(x) \tag{2}$$

where, $0 \le j \le L - 1$ is an integer. Equation 2 implies that gcd($f_i(x)$, g(x)) = 1 and gcd($f_i(x)$, a(x)) = 1 where gcd stands for greatest common divisor. Integer j in equation 2 is known as exponent of f(x). The set of $2^m - 1$ non-zero polynomials, $f_j(x)$, includes all non-zero polynomials of degree d, $0 \le d < m$, [3]. However, only the subset of zero-delay elements in this set is of our interest.

For convenience and without loss of generality, in the following we drop subscript j from $f_j(x)$ and rewrite equation 2 as,

$$f(x) + a(x)g(x) = x^j \tag{3}$$

Next, divide both sided of (3) by g(x)f(x);

$$\frac{1}{g(x)} + \frac{a(x)}{f(x)} = \frac{x^j}{f(x)g(x)}. \tag{4}$$

Theorem 1 can now be proved by interpreting equation 4 in terms of the periodic sequences generated by linear feedback shift-registers having g(x), f(x), and f(x)g(x) as their characteristic polynomials.

The first term in the left-hand side (LHS) of (4) represents an m-sequence of period L generated by an LFSR having characteristic polynomial g(x) and initially loaded by the unit vector, U. Similarly, the second term in the LHS of (4) stands for a sequence that, after some tail bits, converges to a periodic sequence, F, (of period P) generated by f(x). The number of tail bits is zero when deg[a(x)] < deg[f(x)] = d. In this case, a(x) represents initial state of the shift-register that generates F. a(x)/f(x) always converges to the periodic sequence since according to equation 2, a(x) and f(x) are relatively prime.

The right-hand side (RHS) term in (4) is the modulo-2 sum of the two sequences generated in the LHS of (4) and represents a periodic sequence generated by an LFSR having characteristic polynomial f(x)g(x) and initially loaded with a unit vector, U. The numerator, x^j, is merely a shift operator for the generated periodic sequence. Period, Q, for the sequence generated in the RHS of (4) is least common multiple (lcm) of L and P, Q = lcm(L, P). Hence,

$$\frac{1}{f(x)g(x)} = \frac{h(x)}{1 + x^Q}$$

or

$$f(x)g(x)h(x) = 1 + x^Q, \tag{5}$$

where, in polynomial form, h(x) represents one period of the sequence generated by f(x)g(x). Equation 5 implies that deg[h(x)] = Q – (m + d). That is, the periodic sequence generated by f(x)g(x) includes a block of m+d-1 consecutive zeros followed by a single 1; the m + d = k-dimensional unit vector U. A block of more than m+d-1 consecutive zeros does not exist on the periodic sequence h(x)/(1+x^Q).

According to equations 1 and 4, the k-dimensional unit vector U is modulo-2 sum of two companion extended states on the considered m-sequence and the sequence generated by a(x)/f(x). Therefore, for any polynomial f(x) of degree d < m, a unique characteristic state of order d exists on an m-sequence generated by a primitive polynomial g(x), deg[g(x)] = m, such that its companion satisfies the recurrence relation of f(x).

Theorem 1 can be also proved by analyzing adjacencies of cycles generated by an LFSR with characteristic polynomial $g(x)f(x)$[2]. A special case of Theorem 1, where f(x) = $(1 + x)^i$, for all integers i > 0, was proved somewhere else, [4].

Example 2: Let g(x) = 1 + x + x^4, m = 4, and f(x) = 1 + x + x^2, d = deg[f(x)] = 2. Then, an exhaustive search in the GF(2^4), generated by g(x), and simple algebraic manipulations yields

$$x^{10} = 1 + x + x^2, \quad \text{mod}[g(x)].$$

Specifically,

$$x^{10} = 1 + x + x^2 + (1 + x^2 + x^3 + x^6)(1 + x + x^4) \tag{6}$$

or

$$\frac{1}{1 + x + x^4} + \frac{1 + x^2 + x^3 + x^6}{1 + x + x^2} = \frac{x^{10}}{(1 + x + x^4)(1 + x + x^2)}$$

In terms of (4), a(x) = $1+x^2+x^3+x^6$ and $x^j = x^{10}$. Illustrated in Figure 1 is the sequence S_1, one period of the m-sequence of period L = 15 generated by 1/g(x). After a few tail bits, a(x)/f(x) converges to a periodic sequence, S_2, of period 3. The leftmost terms in S_1 and S_2 are the first generated bits. Bit-by-bit modulo 2 sum of S_1 and S_2 is a periodic sequence of period 15 = lcm(15, 3) and generated by x^{10}/f(x)g(x).

Clock Cycle:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1 =	1	1	1	1	0	**1**	**0**	**1**	**1**	**0**	**0**	1	0	0	0
S_2 =	1	1	1	1	0	**1**	**0**	**1**	**1**	**0**	**1**	1	0	1	1
S_1+S_2 =	0	0	0	0	0	**0**	**0**	**0**	**0**	**0**	**1**	0	0	1	1

Figure 1. One period of the m-sequence S_1 generated by 1/(1+x+x^4), the first 15 bits of sequence S_2 generated by (1+x^2+x^3+x^6)/(1+x+x^2), and S_1 + S_2.

[2] Cycles of an LFSR and their adjacencies are defined in section V.

The underlined unit vector (0, 0, 0, 0, 0, 1) on $S_1 + S_2$ corresponds to the bit-by-bit modulo-2 sum of (1, 0, 1, 1, 0, 0) and (1, 0, 1, 1, 0, 1); the extended state of order d = 2 on S_1 and its companion on S_2, respectively. Therefore, companion of the extended state of order 2 on the m-sequence, (1, 0, 1, 1, 0, 1), satisfies the recurrence relation of $f(x) = 1 + x + x^2$. The block of 10 consecutive zeros appearing at the beginning of $S_1 + S_2$ is due to the shift operator $x^j = x^{10}$ in equation 6. Also, the characteristic state for f(x) appears exactly after the LFSR that generates the m-sequence is clocked j+1 = 11 times.

IV. Exponents of a Characteristic State

Theorem 2. Let an LFSR with characteristic primitive polynomial g(x), deg[g(x)] = m, be initially loaded with the unit vector. Suppose that the characteristic states for polynomials u(x), deg[u(x)] < m and v(x), deg[v(x)] < m, appear on the generated m-sequence exactly after $j_u + 1$ and $j_v + 1$ clock periods, respectively. Then, the characteristic state for a polynomial w(x) = u(x)v(x) appears exactly after $j = j_u + j_v + 1$ modulo(L) clock cycles provided that gcd(g(x), w(x)) = 1.

Proof: Trivially follows from equation 3.

$$u(x) + a_u(x)g(x) = x^{j_u}$$

$$v(x) + a_v(x)g(x) = x^{j_v}$$

Hence,

$$u(x)v(x) = w(x) = x^{(j_u+j_v)\mathrm{modulo}L}, \quad \mathrm{mod[g(x)]} \qquad (7)$$

which can be readily written in the form of equation 4. In equation 7, f(x) is written as product of polynomials u(x) and v(x) and not reduced modulo g(x). Therefore, the degree of f(x) does not necessarily need to be less than the degree of g(x), as assumed in theorem 1.

Theorem 2 illustrates multiplication to addition transformation property of cross-recurrence property of m-sequences; identical to the logarithm property. By induction, theorem 2 can be readily generalized for the case that f(x) is the product of several polynomials provided that gcd(f(x), g(x)) = 1.

Example 3: Consider a binary primitive polynomial of degree m = 4, $g(x) = 1 + x + x^4$ and let $f(x) = 1 + x^3 = (1 + x)(1 + x + x^2)$. In this example, exponents of factors of f(x) can be readily determined algebraically without the need for actually generating the m-sequence or searching in the extended finite field generated by g(x).

First, g(x) = 0 implies that $x^4 = 1 + x$ which is in the form of equation 3. Hence, when initially loading the m-sequence generator with a unit vector, the characteristic state, (1,1,1,1,0), for factor 1+ x appears on the m-sequence after 4 + 1 = 5 clock cycles. In other words, it takes four steps to reach the all one state (1, 1, 1, 1) and one more step to reach the extended state of order one, (1, 1, 1, 1, 0).

Similarly, $g(x) = 1 + x + x^4 = 0$ can be written as $1 = x(1+x)(1+x+x^2)$. Substituting x^4 for 1+x yields $1 = x^5(1+x+x^2)$. Using the fact that in GF(16), $x^{15} = 1$ we have, $x^{10} = 1 + x + x^2$ mod[g(x)], which is the same exponent for the factor $1+x+x^2$ derived in Example 2 by inspection. Hence, characteristic state for the factor $1 + x + x^2$ appears after 10 + 1 = 11 clock cycles and characteristic state for $f(x) = 1 + x^3$, appears on the m-sequence after the LFSR is clocked 4 + 10 + 1 = 15 times.

V. Potential Applications

As potential applications of the cross-recurrence property of m-sequences, introduced in this paper, generation of nonlinear maximal length sequences and a methodology to solve the discrete logarithm problem in finite fields of characteristic two are briefly outlined in the following.

A. Maximal Length Nonlinear Sequence Generation

A well-known procedure to generate maximal length nonlinear sequences is to analyze cycle structure of an LFSR and join the adjacent cycles in the state diagram of the LFSR, [1]. Two cycles are disjoint if they don't have a common state. Two disjoint cycles C_1 and C_2 are adjacent if companion of one of states on C_1 belongs to C_2. Cycles C_1 and C_2 can be joined to a single cycle when predecessors of the companion states are interchanged, [1]. For an example of such non-linear sequence generation technique see [5] where adjacencies of cycles of an LFSR with tap connection $g(x)(1+x)^2$ were analyzed and used to generate a large class of non-linear sequences. The sequences constructed in [5] however, are partially linear; consist of long strings of consecutive bits that can be generated by short LFSRs. Using the cross recurrence property of m-sequences, complex nonlinear sequences can be generated by joining cycles of an LFSR with characteristic polynomial

$$G(x) = g(x)\prod_i b_i(x)$$

where, g(x) is a primitive polynomial and $b_i(x)$ are low degree polynomials.

B. The Discrete Logarithm Problem in GF(2^m)

In the context of cross-recurrence property of m-sequences, presented in this paper, the discrete logarithm problem is to find an answer to the following question. Beginning from the unit vector, after how many shift-register clocks the extended state of order d, satisfying recurrence relation of a given polynomial f(x), deg[f(x)] = d, appears on an m-sequence generated by a primitive polynomial, g(x), of degree m? In terms of equations 3 and 4, the discrete logarithm problem is to find exponent j when polynomials g(x) and f(x) are known.

The above definition of discrete logarithm is given for convenience and illustrative purposes. In practice however, what is known is an extended state of order d on the m-sequence and not the polynomial f(x). Nonetheless, for a given extended state, polynomial f(x) can be determined from the Massey algorithm, [6].

The index calculus algorithm, extensively examined in [2], is a well-known probabilistic approach to solve the discrete logarithm problem. In principle, the algorithm consists of two main stages. In the first stage, a look-up table is established to list exponents, j, for as many low degree irreducible polynomials as practical (in terms of required memory and computational effort). This stage of the algorithm is the most computationally intensive however, clever methods are known to expedite the look-up table generation, [7]. In the next stage, the polynomial f(x), derived by Massey algorithm for a given extended state of order d, is examined for smoothness. A polynomial is smooth if it can be written as the product of several irreducible polynomials of low degree. Using the results of Theorem 2, which transforms multiplication to addition, exponent j for f(x) can be determined from exponents of its factors available from the look-up table.

It is well known that low degree polynomials are more likely than high degree polynomials to be smooth, [2]. In many instances however, a polynomial of degree k >> 1 might not be smooth but the characteristic polynomial for the shortest LFSR that generates it (obtained from Massey algorithm) might be smooth.

Example 4. The polynomial 13535 of degree 12, represented in octal, is irreducible, [8, Table C.2]. It can be however, generated by a six-stage LFSR with feedback polynomial f(x) = $1+x^6 = (1 + x)^2(1+x+x^2)^2$. That is, when appearing on an m-sequence, exponent of the extended state 13535 can be readily found if exponents of its factors, 1 + x and $1 + x + x^2$, are known.

VI. References

[1] S. W. Golomb, *Shift-Register Sequences*, Revised Edition, Aegean Park Press, 1982.

[2] A. M. Odlyzko, "Discrete logarithm in finite fields and their cryptographic significance", http://www.dtc.umn.edu/~odlyzko/doc/arch/discrete.logs.pdf.

[3] S. Lin and D, J, Costello, Jr., Error *Control Coding: Fundamentals and Applications*. Prentice-Hall, New Jersey, 1983.

[4] F. Hemmati, ``A New Property for PN Sequences", Proceedings of the Third SIAM Conference on Discrete Mathematics, Clemson, SC, May 1986.

[5] F. Hemmati: "A large class of nonlinear shift-register sequences". IEEE Transactions on Information Theory 28(2): 355-359 (1982).

[6] J. L. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Transactions on Information Theory, January 1969.

[7] D. Coppersmith. "Fast evaluation of discrete logarithms in fields of characteristic two", IEEE Transactions on information Theory, 1984.

[8] W.W. Peterson and E.J. Weldon, Jr., Error-Correcting Codes, 2nd edition, MIT Press: Cambridge, Mass., 1972,