PROOF OF MASSEY'S CONJECTURED ALGORITHM

Cunsheng Ding
Department of Applied Mathematics
Northwest Telecommunication Engineering Institute
Xian, People's Republic of China

ABSTRACT: Massey's conjectured algorithm for multi-sequence shift register synthesis is proved, and its suitability for the minimal realization of any linear system is also verified.

I . INTRODUCTION

It is well known that the SLFSR(shortest linear feedback shift register) synthesis of single-sequence is of great importance in practice(1)(2). The Berlekamp-Massey algorithm gives an efficient one(2). The problem of synthesizing multi-sequence with LFSR has been given much concern by many scholars in information and control society. J.L. Massey gave a conjectured algorithm for the SLFSRsynthesis of multi-sequence in 1972. In 1985 Fen Gweiliang and K.K. Tzeng also gave another one(3). In this paper we are going to prove Massey's conjectured algorithm, and verify that it is an universal one and is suited for the minimal realization of any linear system.

II . PROOF OF MASSEY'S CONJECTURED ALGORITHM

Let $B_i = a_{i1} \cdots a_{iN}$, $i=1, \ldots, M$, be M sequences of length N in the field F and $S_i=(a_{1i}\ a_{2i} \cdots a_{Mi})^t$, $S=(B_1\ B_2 \cdots B_M)^t$, $S^i=S_1 \ldots S_i$. Then the Massey's conjectured algorithm in Fig. 1 can be stated as

MASSEY'S CONJECTURE: Assume that (f_i, l_i) is the SLFSR which generates S^i, and $d_i=f_i(S^{i+1})$ is the i^{th} discrepancy, $i=0, \ldots, n$. Then

(i) if $d_n=0$, then $l_{n+1}=l_n$ and $f_{n+1}=f_n$.

(ii) if $d_n \neq 0$, and is a linear combination of d_i, $i=0, \ldots, n-1$, let $d_{k_1}, \ldots d_{k_r}$ be a basis of $d_i : 0 \leq i \leq n-1$ such that $\max\{n-k_i+l_{k_i} : 1 \leq i \leq r\}$ is minimal and $(k_1, k_2, \ldots, k_r)$ is maximal in alphabetic order. Let

$$d_n = -\sum_{i=1}^{r} u_i d_{k_i}, \quad I = \{i : u_i \neq 0, 1 \leq i \leq r\}$$

then $l_{n+1} = \max\{l_n, \max n-k_i+l_{k_i} : i \in I\}$, $f_{n+1} = f_n + \sum_{i=1}^{r} u_i x^{n-k_i} f_{k_i}$

C.G. Guenther (Ed.): Advances in Cryptology - EUROCRYPT '88, LNCS 330, pp. 345-349, 1988.
© Springer-Verlag Berlin Heidelberg 1988

(iii) if d_n is not a linear combination of d_i, i=0, ... , n-1, then $l_{n+1} = n+1$ and f_{n+1} can be any polynomial in F[x] of degree n+1.

First, we give some notations and simple results:

Let $f_i = 1+f_{i,1}x + \cdots + f_{i,l_i}x^{l_i}$, and $ff_i=(0 \cdots 0\ f_{i,1} \cdots f_{i,l_i}\ 1\ 0 \cdots 0)$ be a vector of length n+1. Denote $D_{n+1}=(d_0\ d_1 \cdots d_n)^t$, $A_{n+1}=(s_1\ s_2 \cdots s_{n+1})^t$ and $F_{n+1}=(ff_0\ ff_1 \cdots ff_n)^t$. Then it is easy to know that

(i) F_{n+1} is a lower triangular matrix, and is invertable.

(ii) $D_{n+1} = F_{n+1} A_{n+1}$, $A_{n+1} = G_{n+1} D_{n+1}$.

where $G_{n+1} = F_{n+1}^{-1}$, and is also a lower triangular matrix.

Let us split the matrices F_{n+1}, G_{n+1}, D_{n+1} and partition them by writing

$$F_{n+1} = \begin{bmatrix} F_n & 0 \\ r_n & 1 \end{bmatrix} \qquad G_{n+1} = \begin{bmatrix} G_n & 0 \\ g_n & 1 \end{bmatrix} \qquad D_{n+1} = \begin{bmatrix} D_n \\ d_n \end{bmatrix}$$

Define matrix $U_{(n-L+1)\times(n+1)}$ as

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & u_L & \cdots & u_1 & 1 \\ 0 & 0 & \cdots & u_L & \cdots & u_1 & 1 & 0 \\ \vdots & \vdots & & \vdots & \ddots & & & \vdots \\ 0 & u_L & \cdots & u_1 & 1 & 0 & \cdots & 0 \\ u_L & \cdots & & 1 & 0 & 0 & \cdots & 0 \end{bmatrix} = \begin{bmatrix} B & & & 1 \\ & & & \\ & & & \\ U_{(n-L)\times n} & & & 0 \end{bmatrix}$$

where $B=(0 \cdots 0\ u_L \cdots u_1)^t$, $0 = (0 \cdots 0)^t$. By definition, it is apparent that the following theorem 1 holds.

Theorem 1. Let $f(x) = 1 + u_1x + \cdots + u_Lx^L$ (L<n+1), then (f,L) generates S^{n+1} if and only if $U_{(n-L)\times(n)}G_nD_n = 0$ and $BG_nD_n + g_nD_n + d_n = 0$.

Theorem 2. If (f,L) can generate S^{n+1}, L<n+1, then there must exist a vector u such that

$$f = f_n + \sum_{i=0}^{n-1} u_i x^{n-i} f_i, \quad d_n = -uD_n = -\sum_{i=0}^{n-1} u_i d_i$$

Theorem 3. Assume that (f_i,L) is the SLFSR which generates S^i, i=0, ... , n. Then $l_{n+1}=n+1$ if and only if d_n is not a linear combination of d_i, i=0, ... , n-1.

Theorem 4. Assume that $g = f_n + \sum_{i=1}^{s} u_i x^{n-k_i} f_{k_i}$, $u_i \neq 0$, i=1, ... , s. Let l_i' be the shortest L such that (f_i,L) can generate S^i. If (g,L) generates

S^{n+1}, then we have

$$L \geq \max\{l'_n, n-k_1+l'_{k_1}, \ldots, n-k_s+l'_{k_s}\} = \max\{l_n, n-k_1+l_{k_1}, \ldots, n-k_s+l_{k_s}\}$$

In order to prove theorem 4, we now prove the following lemma:

Lemma: Assume $G = f_m + u_1 x^{m-k_1} f_{k_1}$, $u_1 \neq 0$, $k_1 < m$, and (f_m, l_m), (f_{k_1}, l_{k_1}) are the SLFSR's which generate S^m and S^{k_1} respectively, then if (g,L) generate S^{m+1}, we have

$$L \geq \max\{l'_m, m-k_1+l'_{k_1}\} = \max\{l_m, m-k_1+l_{k_1}\}$$

Proof: From the definition of l'_m and l_m, we obtain that $l'_m = l_m$ and $l'_{k_1} = l_{k_1}$. Because $L \geq l_m$, so $L \geq l_m = l'_m$. Suppose $l'_m \leq L < m-k_1+l'_{k_1}$. Let j be the last j such that $f_{k_1,j} \neq 0$.

1) if $j+m-k_1 \leq l'_m$, because $L \geq l'_m$, so $L-m+k_1 \geq l'_m-m+k_1 \geq j$. Put $LL = L-m+k_1$ and $h(x) = 1+h_1x+\ldots+h_jx^j$, where $h_i = f_{k_1,i}$, $i = 1, \ldots, j$. Then

$$g(x) = f_m + u_1 x^{m-k_1} h(x), \quad j \leq LL < l'_{k_1}.$$

Because (g,L) generates S^m and $L \geq l_m$, so $g(S^m) = \ldots = g(S^{L+1}) = 0$, and $f(S^m) = \ldots = f(S^{L+1}) = 0$. Thus $h(S^{k_1}) = \ldots = h(S^{LL+1}) = 0$. This meas that $(h, LL) = (g, LL)$ generate S^{k_1}, but $LL < l'_{k_1}$. It is contrary to the minimality of l'_{k_1}, hence $L \geq m-k_1+l'_{k_1} = \max\{l'_m, m-k_1+l'_{k_1}\} = \max\{l_m, m-k_1+l_{k_1}\}$.

2) if $j+n-k_1 > l'_m$, regard $g(x)$ and $f_m + x^{m-k_1} f_{k_1}$ as polynomials of degree m, $m \leq n$. Then the degenerating terms of $f_m + x^{m-k_1} f_{k_1}$ is $m-(m-k_1+j)$, so $m-L \leq m-(m-k_1+j)$. Put $LL = L-m+k_1$, then $j \leq LL < l'_{k_1}$. For the same reason we know that $(h(x), LL)$ generates S^{k_1}, but $LL < l'_{k_1}$. This is also contrary to the minimality of l'_{k_1}. Thus $L \geq \max\{l'_m, m-k_1+l'_{k_1}\} = \max\{l_m, m-k_1+l_{k_1}\}$.

PROOF OF THEOREM 4: By using the above lemma and induction on s, it is not difficult to see that Theorem 4 is true.

Theorem 5. Let (f_i, l_i) be the SLFSR which generate S^i, and $d_i = f_i(S^{i+1})$, $i = 0, \ldots, n-1, n$. If $d_n (\neq 0)$ can be expressed as a linear combination of d_i, $i = 0, \ldots, n-1$, say $d_n = -uD_{n-1} = -\sum u_i d_i$. Let $I_u = \{0 \leq i \leq n-1 : u_i \neq 0\}$. Put

$$l_{n+1} = \min_{\substack{u \\ d_n = -uD_n}} \max\{l_n, n-i+l_i : i \in I_u\} \qquad \ldots (\&)$$

$$f_{n+1} = f_n + \sum_{i=0}^{n-1} u'_i x^{n-i} f_i$$

where $u' = (u'_0, \ldots, u'_{n-1})$ is the vector which makes the right side of (&) take its minimal value. Then (f_{n+1}, l_{n+1}) is a shortest LFSR that generate S^{n+1}.

Proof: Let L denote the right side of (&). It is obvious that $l_{n+1} \leq L$. Let (f, l_{n+1}) is a SLFSR that generate S^{n+1}, and $l_{n+1} < n+1$. By theorem 2 there must exist a vector u such that

$$f = f_n + \sum_{i=0}^{n-1} u_i x^{n-i} f_i, \; d_i = -uD_n = -\sum_{i=0}^{n-1} u_i d_i.$$

Then theorem 4 tell us that $l_{n+1} \geq \max\{l_n, n-k_i+l_{k_i} : i \in I_u\} \geq L$, therefore $l_{n+1} = L$. Thus (f_{n+1}, l_{n+1}) is a SLFSR which generate S.

From the base chosen in Massey's algorithm and Theorem 5 we can easily conclude that the part (i i) in Massey's algorithm is true. Part (iii) has been proved in theorem 3. Part (i) is apparently true. Thus we have comletely proved Massey's conjectured algorithm until now.

Let V be a vector space over the field F, $S = s_1 \ldots s_n$ be a vector sequence of length n. the problem of finding a pair $(f_n(x), l_n)$ such that (f_n, l_n) generates S^n and l_n is minimal is refered to as the problem of minimal realization for vector sequence.

Notice that the proofs of all the theorems and lemma is independent of what the s_i's are, but only require that s_i's belong to a vector space over F. So all the results are true for vector sequence. This means that Massey's algorithm is an universal one, it is suited for the minimal realization of any linear system. We now give some special cases of the universal algorithm:

1) If $V = F$, then it is the B-M algorithm.

2) If $V = F^m$, then it is the Massey's one for multi-sequence LFSR synthesis.

3) If $V = F_{n \times n}$, then it gives a minimal realization algorithm for matrix sequence.

4) If $F = GF(q)$, $V = GF(q^m)$, then it gives a minimal realization algorithm for the sequence in $GF(q^m)$ over $GF(q)$.

ACKNOWLEDGMENT

The author wishes to thank Prof. Xiao Guozhen for his guidance. Also much thanks to Shan Weijuan, Guo Baoan and the people in the 'Seminar for the Theory of Coding and Cryptology' for their helpfull suggestions.

REFERENCES

(1) Xiao Guozheng et.al, 'Pseudorandom sequences and their applications'. The National Defense Industry Press of China.
(2) J.L. Massey, 'Shift-register synthesis and BCH decoding'. IEEE Trans. Infor. Theory, Vol. IT-15, Jan. 1969.
(3) Feng Gueilian and K.K. Tzeng, 'A Iterative Algorithm for Multi-sequences Synthesis with Shortest LFSR'. Scientia Sinica(Science in China), A. August 1985.

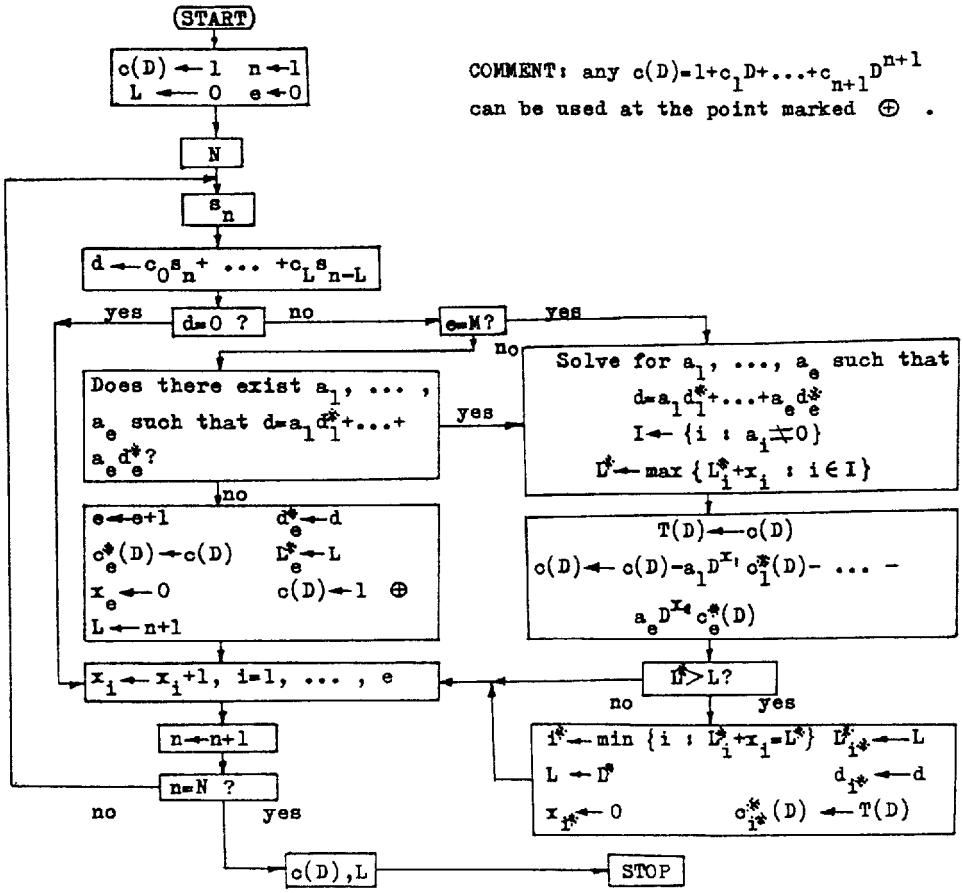

Fig.1 Massey's Conjectured Algorithm for Multi-sequence Shift Synthesis.