MATH. SCAND. 33 (1973), 13–17

LINEAR RECURRENCE IN BOOLEAN RINGS. PROOF OF KLØVE'S CONJECTURE

JOHANNES MYKKELTVEIT and ERNST S. SELMER

In the preceeding paper [2], to which we had access in manuscript, Kløve puts forward a conjecture on linear recurring sequences in Boolean rings. We shall prove this conjecture. The representation of ring elements by vectors was suggested by Mykkeltveit, and the reformulation of the conjecture by Selmer.

We shall follow Kløve's notation throughout.

1. Reformulation of the conjecture.

We define

$$m_1 \subset m_2 \quad \text{iff} \quad \beta_i(m_1) \leqq \beta_i(m_2) \text{ for all } i\,,$$

that is, *iff the binary representation of* m_2 *contains at least the same* 1*'s as that of* m_1. Then Kløve's conjecture can be written

$$f_m(X) \mid h_m(X) = \operatorname{lcm}_{\mu \subset m} Q_\mu(X)\,. \tag{1.1}$$

In the recurrence relation

$$x_n = a_1 x_{n-1} + \ldots + a_r x_{n-r}, \quad n \geqq 0\,, \tag{1.2}$$

we replace some of the a_i's by zero, and are then left with a recurrence

$$x_n = a_{j_1} x_{n-j_1} + \ldots + a_{j_s} x_{n-j_s}, \quad n \geqq 0\,, \tag{1.3}$$

where the coefficients a_{j_i} are independent elements of the given Boolean ring. The choice of coefficients is uniquely determined by the number

$$m = \textstyle\sum_{i=1}^{s} 2^{j_i-1}\,. \tag{1.4}$$

This is constructed from the indices j_i in exactly the same way as Kløve uses to characterize any choice of the original coefficients $a_1,\ldots,a_r$ by a number m.

Received December 8, 1972.

Let $G_m(X)$ be the polynomial in GF[2][X] of least degree associated with the recurrence (1.3). Using all coefficients in (1.2), we see that $G_{2^r-1}(X)$ is the same as Kløve's $F_r(X)$.

If we for the parameters a_{j_i} choose particular values lying in GF[2], then the associated polynomial must be a divisor of $G_m(X)$, hence

$$(1.5) \qquad \operatorname{lcm}_{\mu \subset m} Q_\mu(X) \mid G_m(X) .$$

On the other hand, we must have

$$(1.6) \qquad G_m(X) \mid \operatorname{lcm}_{\mu \subset m} f_\mu(X) ,$$

in analogy with Kløve's formula (4.5). Combining (1.1), (1.5) and (1.6), we see that Kløve's conjecture implies

$$h_m(X) = \operatorname{lcm}_{\mu \subset m} Q_\mu(X) \mid G_m(X) \mid \operatorname{lcm}_{\mu \subset m} f_\mu(X) \mid \operatorname{lcm}_{\mu \subset m} h_\mu(X) = h_m(X) ,$$

and thus

$$(1.7) \qquad G_m(X) = \operatorname{lcm}_{\mu \subset m} Q_\mu(X), \quad 1 \leqq m \leqq 2^r - 1 .$$

Conversely, (1.7) implies that

$$G_m(X) = \operatorname{lcm}_{\mu \subset m} f_\mu(X) = h_m(X) ,$$

and thus $f_m(X) \mid h_m(X)$, which is Kløve's conjecture. This is consequently equivalent to the relation (1.7).

Since we are going to prove it, we state the reformulated conjecture as a

THEOREM. *Let A be a Boolean ring, and consider the linear recurrence*

$$x_n = a_{j_1} x_{n-j_1} + \ldots + a_{j_s} x_{n-j_s}; \qquad a_{j_i}, x_k \in A ,$$

where the coefficients a_{j_i} are independent parameters. Let $G_m(X)$ be the polynomial in GF[2][X] *of least degree associated with this recurrence.*

For the parameters a_{j_i}, we can in $2^s - 1$ ways choose particular values, not all 0, lying in GF[2]. *For each such choice, we get a binary recurrence relation with an associated characteristic polynomial $Q_\mu(X)$. The least common multiple of these polynomials is then just $G_m(X)$.*

Formulated this way, the truth of Kløve's conjecture appears very likely indeed. It does, however, seem hard to prove by the method used in Kløve's paper.

2. Proof of the theorem.

Following Berlekamp [1, p. 365], we shall represent the elements $a_{j_i} \in A$, $i = 1, 2, \ldots, s$, by binary (column) vectors $\mathbf{a}_{j_i}$ of dimension 2^s. Addition of such vectors is component-wise modulo 2, and *also multiplication is performed component-wise.* Any product of elements a_{j_i} shall be represented by the product of the corresponding vectors $\mathbf{a}_{j_i}$. The vectors with all components 0 or all 1 are denoted $\mathbf{0}$ and $\mathbf{1}$, respectively. The fundamental relations $\mathbf{a}^2 = \mathbf{a}$ and $2\mathbf{a} = \mathbf{0}$ of a Boolean ring clearly hold.

To fix the ideas, we illustrate the choice of vectors $\mathbf{a}_{j_i}$ for $s = 3$ in Table (2.1). We number both rows and columns from 0 to $2^s - 1 = 7$. Then the digits of row ϱ and column $1, 2, 3 = s$ form the binary representation, in reverse order, of the number ϱ. Equivalently, we can say that the components of $\mathbf{a}_{j_i}$ are grouped in alternating blocks of 2^{i-1} 0's and 2^{i-1} 1's.

Table (2.1)

$\mathbf{1}$	$\mathbf{a}_{j_1}$	$\mathbf{a}_{j_2}$	$\mathbf{a}_{j_3}$	$\mathbf{a}_{j_1}\mathbf{a}_{j_2}$	$\mathbf{a}_{j_1}\mathbf{a}_{j_3}$	$\mathbf{a}_{j_2}\mathbf{a}_{j_3}$	$\mathbf{a}_{j_1}\mathbf{a}_{j_2}\mathbf{a}_{j_3}$
1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	1	0	1	0	0	0
1	0	0	1	0	0	0	0
1	1	0	1	0	1	0	0
1	0	1	1	0	0	1	0
1	1	1	1	1	1	1	1
$\nu = 0$	1	2	4	3	5	6	7

Each product

$$\textstyle\prod_{i=1}^{s} \mathbf{a}_{j_i}^{\alpha_i}, \qquad \alpha_i = 0, 1 ,$$

can in the usual way (cf. (1.4)) be characterized by the number

$$\nu = \textstyle\sum_{\alpha_i = 1} 2^{i-1} ,$$

which is given below the vectors in (2.1). From the choice of $\mathbf{a}_{j_i}$, it follows easily that the column vector corresponding to ν has the first ν components $= 0$ and the $(\nu + 1)$st component $= 1$. By permuting columns, we can therefore transform the matrix of (2.1) into a matrix $\mathscr{T}$ with 1's along the main diagonal and 0's above this diagonal. The vectors of (2.1) are thus *linearly independent.*

Incidentally, it can be shown that the complete distribution of 0's and 1's among the elements $t_{\lambda,\nu}$ of $\mathscr{T}$ is determined by

$$t_{\lambda,\nu} = 1 \Leftrightarrow \nu \subset \lambda \,. \tag{2.2}$$

Because of the linear independence, any binary vector $\boldsymbol{x}$ of dimension 2^s is uniquely determined as a (binary) linear combination of the vectors of (2.1). No proper binary polynomial in these vectors can therefore vanish identically. This ensures that the independence of the ring elements a_{j_i} is *retained* by the vector representation chosen.

In the recurrence (1.3), the initial elements $x_{-1}, x_{-2}, \ldots$ could of course be ring elements different from 0, 1 or polynomials in the coefficients a_{j_i}. This would necessitate representation by vectors of dimension 2^σ with $\sigma > s$. However, as pointed out by Kløve, we get the same period and the same "minimal" associated polynomial $G_m(X)$ if we use the initial values $x_{-1}=1, x_{-2}=x_{-3}=\ldots=0$. In the notation of Selmer [3], the resulting recurring sequence is the "impulse response sequence", IRS. (In a feedback shift register, this sequence results from applying a single pulse to an empty register.)

In the vector representation of the recurrence (1.3), we can consequently use the initial vectors $\boldsymbol{x}_{-1}=\boldsymbol{1}$, $\boldsymbol{x}_{-2}=\boldsymbol{x}_{-3}=\ldots=\boldsymbol{0}$. Any vector $\boldsymbol{x}_n$ is then a binary polynomial in $\boldsymbol{a}_{j_1}, \ldots, \boldsymbol{a}_{j_s}$, and vectors of dimension 2^s will suffice.

Again to fix the ideas, we illustrate the vector form of (1.3) for $s=2$:

$$\begin{Bmatrix} x_n^{(0)} \\ x_n^{(1)} \\ x_n^{(2)} \\ x_n^{(3)} \end{Bmatrix} = \begin{Bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{Bmatrix} \begin{Bmatrix} x_{n-j_1}^{(0)} \\ x_{n-j_1}^{(1)} \\ x_{n-j_1}^{(2)} \\ x_{n-j_1}^{(3)} \end{Bmatrix} + \begin{Bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{Bmatrix} \begin{Bmatrix} x_{n-j_2}^{(0)} \\ x_{n-j_2}^{(1)} \\ x_{n-j_2}^{(2)} \\ x_{n-j_2}^{(3)} \end{Bmatrix} \,, \quad n \geqq 0 \,. \tag{2.3}$$

Clearly $x_n^{(0)}=0$ for $n \geqq 0$. The remaining $\{x_n^{(\lambda)}\}_{n \geqq 0}$ for $1 \leqq \lambda \leqq 2^{s-1}$ are binary sequences of the type IRS, determined by the recurrence relations described in the theorem, with characteristic polynomials $Q_\mu(X)$, $\mu \subset m$, where m is given by (1.4). Since the characteristic polynomial is also the "minimum polynomial" (cf. Selmer [3]) of an IRS in GF[2], their least common multiple is just the $G_m(X)$ of the theorem. This proves the theorem.

To stress that the $\{x_n^{(\lambda)}\}$ of (2.3) are impulse response sequences, let us denote them by $\{Z_n^{(\mu)}\}$ (in the notation of Selmer [3]). The upper index μ indicates the characteristic polynomial $Q_\mu(X)$.

The only vector of (2.1) with an *odd* number of components 1 is the last one, corresponding to the product of all vectors $\boldsymbol{a}_{j_i}$. Hence a vector $\boldsymbol{x}_n$ will contain this product as an addend iff the vector has an odd number of components 1, that is, iff

$$\sum_{\mu \subset m} Z_n^{(\mu)} \equiv 1 \pmod 2 . \tag{2.4}$$

We now return to the recurrence (1.3) in the ring A, where (2.4) is the condition for x_n to contain the product of all the coefficients as an addend. Since the deleted coefficients in the transition from (1.2) to (1.3) will not influence the occurrence of this product, the condition (2.4) applies to the complete recurrence (1.2) as well. In this recurrence, with the IRS, Kløve denotes the coefficient of $a_{j_1}a_{j_2}\ldots a_{j_s}$ by $T(m,n)$, where m is given by (1.4). Comparing with (2.4), we get the interesting formula

$$T(m,n) \equiv \sum_{\mu \subset m} Z_n^{(\mu)} \pmod 2 , \quad n \geqq 0 , \tag{2.5}$$

where the summation is taken over all IRS for $\mu \subset m$.

This formula should be compared with Kløve's formula (4.4), which contains indices $<n$ on the right hand side. This fact seems to make Kløve's method less efficient than the vector method used above.

In Kløve's notation, $f_m(X)$ is the minimum polynomial in $\mathrm{GF}[2][X]$ associated with the binary sequence $\{T(m,n)\}_{n \geqq 0}$. This means that (2.5) yields an immediate proof of Kløve's conjecture in the unmodified version (1.1).

REFERENCES

1. E. R. Berlecamp, *Algebraic coding theory*, McGraw-Hill, New York 1968.
2. T. Kløve, *Linear recurring sequences in Boolean rings*, Math. Scand. 33 (1973), 5–12.
3. E. S. Selmer, *Linear recurrence relations over finite fields*, Mimeographed lecture notes, Bergen 1966.

UNIVERSITY OF BERGEN, NORWAY