MATH. SCAND. 33 (1973), 5–12

LINEAR RECURRING SEQUENCES IN BOOLEAN RINGS

TORLEIV KLØVE

1.

A Boolean ring A is a commutative ring with unit satisfying $a^2 = a$ and $2a = 0$ for all $a \in A$. We note that $\mathrm{GF}[2] = \{0, 1\}$ is a subring of A.

A *linear recurring sequence* of *order* r in A is a sequence $\{x_n\}_{n \geqq -r}$ of elements from A satisfying

$$x_n = a_1 x_{n-1} + \ldots + a_r x_{n-r} \tag{1.1}$$

for all $n \geqq 0$. We call $x_{-r}, \ldots, x_{-1}$ the *initial values* and $a_1, \ldots, a_r$ (which are again elements of A) the *coefficients* of the linear recurring sequence.

A sequence $\{x_n\}$ of elements from A is *periodic* if there exist integers $p > 0$ and N such that

$$x_{n+p} = x_n \tag{1.2}$$

for all $n \geqq N$. We call p a *general period*. The least general period is called *the period* of the sequence. Note that the period divides any general period.

Every linear recurring sequence in a Boolean ring is periodic. This is implied by a general theorem proved in [1]. Now, suppose that $a_1, \ldots, a_r$ are independent parameters (i.e. they are having no non-trivial relations between them). Let $P(r)$ be the period of the sequence $\{x_n\}$ satisfying (1.1) with initial values $0, \ldots, 0, 1$. The period of any linear recurring sequence of order r always divides the period of the linear recurring sequence with the same coefficients and with initial values $0, \ldots, 0, 1$ (cf. Selmer [2]. The argument given therein is valid in any ring). Hence $P(r)$ is a general period of any linear recurring sequence of order r in A. We shall prove the following theorem (where lcm denotes least common multiple and $[x]$ denotes the greatest integer $\leqq x$).

THEOREM. (i) *There exists a least positive integer $P(r)$ such that, for any linear recurring sequence $\{x_n\}$ of order r, we have $x_{n+P(r)} = x_n$ for all $n \geqq 0$.*

(ii) *For $r \geqq 1$ we have*

$$P(r) = 2^{\nu(r)} \operatorname{lcm}_{1 \leqq j \leqq r} \{2^j - 1\} ,$$

Received June 5, 1972.

where

$$v(r) = -[-\log_2 r] \quad \textit{for} \quad 1 \leqq r \leqq 6 ,$$
$$r \leqq 2^{v(r)} < 2r[\tfrac{1}{2}(r+1)] \quad \textit{for} \quad r \geqq 1 .$$

2.

To each relation (1.1) we associate a polynomial in $A[X]$, namely

$$X^r + a_1 X^{r-1} + \ldots + a_r , \tag{2.1}$$

and vice versa. If the sequence $\{x_n\}$ satisfies (1.1), then (2.1) is said to be associated with $\{x_n\}$.

If $a_1,\ldots,a_r$ are independent and $\{x_n\}$ satisfies (1.1) with initial values $0,\ldots,0,1$, then $\{x_n\}$ satisfies $x_{n+P(r)} = x_n$. Hence $X^{P(r)}-1$ is associated with $\{x_n\}$. Let $F_r(X)$ be the polynomial in GF[2][X] of least degree associated with $\{x_n\}$.

The number of irreducible polynomials of degree n in GF[2][X] is (cf. Selmer [2 p. 13])

$$I(n) = n^{-1} \textstyle\sum_{cd=n} \mu(c) 2^d . \tag{2.2}$$

Let $\varphi_{n\nu}(X)$, $n \geqq 1$, $1 \leqq \nu \leqq I(n)$ be these irreducible polynomials. In particular, the two of degree 1 are $\varphi_{11}(X) = X+1$ and $\varphi_{12}(X) = X$. In the following we shall not be interested in $\varphi_{12}(X)$. Define $I^*(n)$ by

$$I^*(1) = 1; \quad I^*(n) = I(n) \quad \text{for} \quad n > 1 .$$

Let

$$F_r(X) = \textstyle\prod_{n=1}^{\infty} \prod_{\nu=1}^{I^*(n)} \varphi_{n\nu}(X)^{\varrho(r;n,\nu)} . \tag{2.3}$$

We prove the following main lemma.

Lemma 1. (i) *For* $1 \leqq r \leqq 6$ *we have*

$$\varrho(r;n,\nu) = [r/n] \quad \textit{for} \quad n \geqq 1,\ 1 \leqq \nu \leqq I^*(n) .$$

(ii) *For* $r \geqq 1$ *we have*

$$[r/n] \leqq \varrho(r;n,\nu) \leqq [r/n][\tfrac{1}{2}(r+1)] \quad \textit{for} \quad n \geqq 1,\ 1 \leqq \nu \leqq I^*(n) .$$

In particular $\varrho(r;n,\nu) = 0$ *for all* $n > r$.

Part (ii) of the theorem is an immediate consequence of this lemma and the theorems IV. 5, p. 82 and IV. 6, p. 84 of Selmer [2].

3.

In this section we prove the lower bound for $\varrho(r;n,\nu)$ and in section 4 we prove the upper bound. In section 5 we take a closer look at $F_r(X)$ for $r \leqq 6$ and make a conjecture on the values of $\varrho(r;n,\nu)$ for general r.

If we for the parameters a_i choose particular values lying in GF[2], then the associated polynomial must be a divisor of $F_r(X)$. If $1 \leqq n \leqq r$ and $1 \leqq \nu \leqq I^*(n)$ then

$$\varphi_{n\nu}(X)^{[r/n]}(X+1)^{r-n[r/n]}$$

is such an associated polynomial. Hence, in particular

$$\varphi_{n\nu}(X)^{[r/n]} \mid F_r(X) . \tag{3.1}$$

This proves that $\varrho(r;n,\nu) \geqq [r/n]$.

4.

For m a positive integer put

$$\lambda(m) = [\log_2 m] , \tag{4.1}$$

and define $\beta_i(m)$ for $m \geqq 0$, $i \geqq 1$ by

$$m = \textstyle\sum_{i=0}^{\infty} \beta_{i+1}(m) 2^i \tag{4.2}$$

where $\beta_i(m) \in \{0,1\}$. Then for $m \geqq 1$, $\beta_{\lambda(m)+1}(m) = 1$ and $\beta_i(m) = 0$ for $i > \lambda(m)+1$. Let $\tau(m)$ be the number of binary 1's in m (that is $\tau(m) = \sum_{i=1}^{\infty} \beta_i(m)$).

Now let, $a_1, \ldots, a_r$ be independent and let $\{x_n\}$ be a sequence satisfying (1.1) with initial values $0,\ldots,0,1$. Applying (1.1) repeatedly we get x_n expressed as a polynomial in $a_1,\ldots,a_r$. The terms of this polynomial are of the form $C\, a_1^{\beta_1} \ldots a_r^{\beta_r}$ where $C, \beta_1, \ldots, \beta_r \in \{0,1\}$ since $2a = 0$ and $a^2 = a$ for all $a \in A$. Hence

$$x_n = \textstyle\sum_{m=0}^{2^r-1} T(m,n) a_1^{\beta_1(m)} \ldots a_r^{\beta_r(m)} \tag{4.3}$$

where $T(m,n) \in \{0,1\}$. Substituting in (1.1) we get

$$\textstyle\sum_{m=0}^{2^r-1} T(m,n) a_1^{\beta_1(m)} \ldots a_r^{\beta_r(m)} = \sum_{j=1}^{r} \sum_{m=0}^{2^r-1} T(m,n-j) a_j\, a_1^{\beta_1(m)} \ldots a_r^{\beta_r(m)} .$$

Equating coefficients we get, for $n \geqq 0$,

$$T(m,n) \equiv \textstyle\sum_j \{T(m,n-j) + T(m-2^{j-1}, n-j)\} , \tag{4.4}$$

where the summation is over all j satisfying $1 \leqq j \leqq \lambda(m)+1$ and $\beta_j(m) = 1$. The congruence $\equiv$ is modulo 2. The initial values of $T(m,n)$ are

$$\begin{aligned} T(m,n) &= 0 \quad \text{for} \quad \text{all } m \text{ if } n < -1 ; \\ T(m,-1) &= 1 \quad \text{for} \quad m = 0 , \\ &= 0 \quad \text{for} \quad m > 0 . \end{aligned}$$

Note that $T(0,n)=0$ for $n \geqq 0$.

It is clear from the periodicity of $\{x_n\}$ that $\{T(m,n)\}$ is periodic in n (m being fixed). Let $f_m(X)$ be the polynomial in $\mathrm{GF}[2][X]$ of least degree associated with $\{T(m,n)\}$. Then

$$F_r(X) \mid \operatorname{lcm}_{1 \leqq m \leqq 2^r - 1} f_m(X) . \tag{4.5}$$

Let

$$Q_m(X) = X^{\lambda(m)+1} + \beta_1(m) X^{\lambda(m)} + \ldots + \beta_{\lambda(m)}(m) X + 1 . \tag{4.6}$$

Let D denote the set of integers j satisfying $1 \leqq j \leqq \lambda(m)+1$ and $\beta_j(m)=1$. With this notation we prove the following lemma.

LEMMA 2. *For* $m \geqq 1$ *we have*

$$f_m(X) \mid Q_m(X) \operatorname{lcm}_{j \in D} f_{m-2^{j-1}}(X) , \tag{4.7}$$

PROOF. If the linear recurrence relation associated with the lcm of (4.7) is applied to (4.4), all the terms $T(m-2^{j-1}, n-j)$ are cancelled. We are left with the linear recurrence relation associated with the polynomial to the right of $\mid$ in (4.7), applied to $\{T(m,n)\}$.

Define g_m recursively by

$$\begin{cases} g_{2^\alpha}(X) = Q_{2^\alpha}(X) \quad \text{for} \quad \alpha = 0,1,\ldots, \\ g_m(X) \;=\; Q_m(X) \operatorname{lcm}_{j \in D} g_{m-2^{j-1}} X . \end{cases} \tag{4.8}$$

We have the following lemma.

LEMMA 3. (i) *If* $\beta_i(m_1) \leqq \beta_i(m_2)$ *for all* $i \geqq 1$ *then* $g_{m_1}(X) \mid g_{m_2}(X)$.

(ii) *For all* $m \geqq 1$ *we have* $f_m(X) \mid g_m(X)$.

(iii) *For all* $r \geqq 1$ *we have* $F_r(X) \mid g_{2^r-1}(X)$.

PROOF. We prove (i) by induction on $\tau(m_2)$. Note that $\tau(m_2) \geqq \tau(m_1)$. First, if $\tau(m_2)=\tau(m_1)$, then $\beta_i(m_2)=\beta_i(m_1)$ for all $i \geqq 1$. Hence $m_2 = m_1$. Next, if $\tau(m_2) > \tau(m_1)$, then there exists at least one j such that $\beta_j(m_2)=1$ and $\beta_j(m_1)=0$. For this j we have

$$\beta_i(m_1) \leqq \beta(m_2 - 2^{j-1}) \quad \text{for all } i \geqq 1 ,$$

and

$$\tau(m_2 - 2^{j-1}) = \tau(m_2) - 1 .$$

By the induction hypothesis $g_{m_1} \mid g_{m_2-2^{j-1}}$. Hence, by (4.8), $g_{m_1} \mid g_{m_2}$.

We prove (ii) by induction on $\tau(m)$. First, by (4.4)

$$T(2^\alpha, n) = T(2^\alpha, n-\alpha-1) .$$

Hence

$$f_{2^\alpha}(X) \mid X^{\alpha+1} - 1 = Q_{2^\alpha}(X) = g_{2^\alpha}(X) .$$

Next, let $\tau(m) > 1$. By the induction hypothesis, $f_{m-2^{j-1}} \mid g_{m-2^{j-1}}$ for all j such that $1 \leqq j \leqq \lambda(m)+1$ and $\beta_j(m) = 1$. Hence $f_m \mid g_m$ by lemma 2 and (4.8)

Finally, (iii) is a consequence of (i), (ii), and (4.5).

Let $\sigma(m;n,\nu)$ and $q(m;n,\nu)$ be the exact powers of $\varphi_{n\nu}(X)$ dividing $g_m(X)$ and $Q_m(X)$ respectively. By (4.8)

$$\sigma(m;n,\nu) = q(m;n,\nu) + \max\nolimits_{j\in D} \sigma(m-2^{j-1};n,\nu) . \tag{4.9}$$

We prove the following lemma.

LEMMA 4. *For* $m \geqq 1, n \geqq 1$ *and* $1 \leqq \nu \leqq I^*(n)$ *we have*

$$\sigma(m;n,\nu) \leqq [(\lambda(m)+1)/n][\tfrac{1}{2}(\tau(m)+1)] .$$

PROOF. The proof is by induction on $\tau(m)$. Let $\tau(m) = 1$, that is $m = 2^\alpha$. Then

$$\sigma(2^\alpha;n,\nu) = q(2^\alpha;n,\nu) \leqq [(\lambda(2^\alpha)+1)/n]$$

by (4.6). Next, let $\tau(m) > 1$. We distinguish between two cases.

Case I.

$q(m;n,\nu) = 0$. Then, by (4.9) ,

$$\begin{aligned} \sigma(m;n,\nu) &= \max\nolimits_{j\in D} \sigma(m-2^{j-1},n,\nu) \\ &\leqq \max\nolimits_{j\in D} \{[(\lambda(m-2^{j-1})+1)/n][\tfrac{1}{2}(\tau(m-2^{j-1})+1)]\} \\ &\leqq [(\lambda(m)+1)/n][\tfrac{1}{2}\tau(m)] . \end{aligned}$$

Case II. $q(m;n,\nu) > 0$. Then $q(m-2^{j-1};n,\nu) = 0$ for all j such that $1 \leqq j \leqq \lambda(m)+1$ and $\beta_j(m) = 1$. For if $q(m-2^{j-1};n,\nu) > 0$, then some positive power of $\varphi_{n\nu}(X)$ would divide

$$Q_m(X) - Q_{m-2^{j-1}}(X) = X^{\lambda(m)+1-j} ,$$

and this is impossible. Hence, by case I,

$$\begin{aligned} \sigma(m;n,\nu) &= q(m;n,\nu) + \max\nolimits_{j\in D} \sigma(m-2^{j-1};n,\nu) \\ &\leqq [(\lambda(m)+1)/n] + [(\lambda(m)+1)/n][\tfrac{1}{2}(\tau(m)-1)] \\ &= [(\lambda(m)+1)/n][\tfrac{1}{2}(\tau(m)+1)] . \end{aligned}$$

The upper bound of lemma 1 (ii) now follows from lemma 3 (iii) and lemma 4 choosing $m=2^r-1$.

Note that the upper bound for $v(r)$ is fixed by the upper bound for $\sigma(2^r-1;1,1)$. Hence it may be improved by giving the exact value of $\sigma(2^r-1;1,1)$. For $r \leqq 14$ this is provided by the following table.

TABLE.

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\sigma(2^r-1;1,1)$	1	2	5	6	10	14	21	22	27	32	42	48	59	70
$r[\frac{1}{2}(r+1)]$	1	2	6	8	15	18	28	32	45	50	66	72	91	98

Let $\pi(m)$ be the period of $\{T(m,n)\}$ and let $N(m)$ be the least non-negativ integer such that $T(m,n+\pi(m))=T(m,n)$ for all $n \geqq N(m)$. To complete the proof of part (i) of the theorem we will show that $N(m)=0$ for all $m \geqq 0$. The proof is by induction on $\tau(m)$.

First, let $\tau(m)=0$; that is $m=0$. Since $T(0,n)=0$ for all $n \geqq 0$ we have $N(0)=0$. Next, let $\tau(m)>0$. Put

$$\pi = \mathrm{lcm}_{j \in D}\, \pi(m-2^{j-1}) .$$

By the induction hypothesis

$$T(m-2^{j-1}, n+\pi) = T(m-2^{j-1}, n)$$

for $n \geqq 0$. Hence, by (4.4),

$$T(m,n+\pi)-T(m,n) \equiv \textstyle\sum_{j\in D} \{T(m,n+\pi-j)-T(m,n-j)\}$$

for $n \geqq \lambda(m)+1$. Rearranging, we get (putting $\lambda=\lambda(m)$)

$$\begin{aligned} T(m,n) \equiv {} & T(m,n+\pi+\lambda+1)+T(m,n+\lambda+1)+T(m,n+\pi) \\ & + \textstyle\sum_{j=1}^{\lambda} \beta_j(m)\{T(m,n+\pi+\lambda+1-j)+T(m,n+\lambda+1-j)\} \end{aligned} \tag{4.10}$$

for $n \geqq 0$. Suppose $N(m)>0$. By (4.10) we get

$$T(m,N(m)-1) = T(m,N(m)+\pi(m)-1) .$$

This contradicts the definition of $N(m)$. Hence $N(m)=0$.

5.

We now look at $f_m(x)$ for $m \leqq 2^6-1$. Let

$$h_{2^\alpha}(X)=Q_{2^\alpha}(X), \quad h_m(X)=\mathrm{lcm}\,\{Q_m(X), \mathrm{lcm}_{j\in D}\, h_{m-2^{j-1}}(X)\} ,$$

where again D is the set of integers j satisfying $1 \leqq j \leqq \lambda(m)+1$ and $\beta_j(m)=1$.

LEMMA 5. *For* $1 \leqq m \leqq 2^6 - 1$ *we have*

$$f_m(X) \mid h_m(X) .$$

This was proved by brute force. We computed $T(m,n)$ for $1 \leqq m \leqq 63$ and $0 \leqq n \leqq 300$ using (4.4). By lemma 2 and induction on $\tau(m)$ we get

$$f_m(X) \mid Q_m(X) \operatorname{lcm}_{j \in D} h_{m-2^j-1}(X) . \tag{5.1}$$

If $Q_m(X)$ is coprime to the lcm factor there is nothing more to prove. Otherwise, we checked that $\{T(m,n)\}$ satisfied the linear recurrence relation associated with h_m for $n \leqq$ the degree of the polynomial to the right of $\mid$ in (5.1).

Now, for $r \geqq 6$ (as in lemma 3),

$$F_r(X) \mid h_{2^r-1}(X) = \operatorname{lcm}_{1 \leqq m \leqq 2^r-1} Q_m(X) = (X+1)^r \prod_{n=2}^{r} \prod_{\nu=1}^{I(n)} \varphi_{n\nu}(X)^{[r/n]} . \tag{5.2}$$

By (3.1), $F_r(X) = h_{2^r-1}(X)$ which proves lemma 1 (i).

On the basis of lemma 5 we put forward the following conjecture.

CONJECTURE. *For* $m \geqq 1$ *we have*

$$f_m(X) \mid h_m(X) .$$

The conjecture implies that $F_r(X) = h_{2^r-1}(X)$ for all $r \geqq 1$ and hence that $v(r) = -[-\log_2 r]$ for all $r \geqq 1$.

As a concluding remark we note that

$$\Delta = \text{degree } h_{2^r-1}(X) = 2^{r+1} - r - 2 .$$

By (5.2) we have

$$\Delta = r + \sum_{n=2}^{r} nI(n)[r/n] = -r + \sum_{n=1}^{r} nI(n)[r/n] .$$

If $J(d)$ is any number theoretic function, then

$$\sum_{p=1}^{r} \sum_{cd=p} J(d) = \sum_{1 \leqq cd \leqq r} J(d) = \sum_{d=1}^{r} J(d) \sum_{d^{-1} \leqq c \leqq rd^{-1}} 1 = \sum_{d=1}^{r} J(d)[r/d] .$$

Hence, by (2.2)

$$\begin{aligned} \Delta + r &= \sum_{n=1}^{r} nI(n)[r/n] \\ &= \sum_{p=1}^{r} \sum_{cd=p} dI(d) = \sum_{p=1}^{r} \sum_{cd=p} \sum_{\gamma\delta=d} \mu(\gamma) 2^{\delta} \\ &= \sum_{p=1}^{r} \sum_{c\gamma\delta=p} \mu(\gamma) 2^{\delta} = \sum_{p=1}^{r} \sum_{\varepsilon\delta=p} 2^{\delta} \sum_{c\gamma=\varepsilon} \mu(\gamma) \\ &= \sum_{p=1}^{r} 2^p = 2^{r+1} - 2 . \end{aligned}$$

REFERENCES

1. Torleiv Kløve, *Periodicity of recurring sequences in rings*, **Math. Scand.** 32 (1973), 165–168.
2. Ernst S. Selmer, *Linear recurrence relations over finite fields*, Mimeographed lecture notes, Bergen 1966.

UNIVERSITY OF BERGEN,
BERGEN, NORWAY