POWERS OF A MATRIX WITH COEFFICIENTS IN A BOOLEAN RING

GERT ALMKVIST

ABSTRACT. The best possible integer $u_n$ such that $f^{u_n} = 1$, if $f$ is an invertible $n \times n$ matrix with coefficients in a Boolean ring, is determined. The period of linear recursive sequences in a Boolean ring (e.g., the trace sequence $\{\text{Tr}(f^k)\}_1^\infty$) is computed.

In Rosenstein [5] it is shown that if $f$ is an invertible $2 \times 2$ matrix over a Boolean ring $A$ with unity, then $f^6 = 1$. In the first part of this paper we compute the best possible integer $u_n$ such that $f^{u_n} = 1$, if $f$ is an invertible $n \times n$ matrix over $A$. As a corollary we get a result by Kløve-Mykkeltveit-Selmer [3], [4] about the period of a linear recursive sequence in $A$.

In the second part of the paper the period of the sequence of polynomials $\det(1 + tf^k)$ is computed. In particular we find that the period of the trace sequence $\text{Tr}(f^k)$ is smaller than the period of the sequence of matrices $f^k$.

Let $M_k = 2^k - 1$ be the $k$th Mersenne number. Define

$$v_n = \text{l.c.m.}(M_1, M_2, \ldots, M_n), \quad u_n = 2^rv_n \quad \text{if} \quad 2^{r-1} < n \leq 2^r.$$

We have $v_1 = 1, v_2 = 3, v_3 = 21, v_4 = 105, v_5 = 3255, v_6 = 9765, v_7 = 1240155, \ldots$, and $u_1 = 1, u_2 = 6, u_3 = 84, u_4 = 420, u_5 = 26040, u_6 = 78120, u_7 = 9921240, \ldots$.

Unless something else is stated, all matrices will have coefficients in an arbitrary Boolean ring $A$. The field with two elements will be denoted by $Z_2$.

Most of the results of this paper were announced at a meeting of the Swedish Society of Mathematicians in Lund, March 1973.

Theorem 1. (a) Let $f$ be an $n \times n$ matrix. Then the sequence $\{f^k\}_1^\infty$ is ultimately periodic and the period divides $u_n$.

(b) The result is best possible in the following sense. Let $B_{n_2}$ be the free Boolean ring on $n^2$ generators $x_{ij}$, $i, j = 1, 2, \ldots, n$. If $f = (a_{ij})$ then $\{f^k\}_1^\infty$ has period $u_n$.

Proof. (a) Let $f = (a_{ij})$ be an $n \times n$ matrix with coefficients in $A$. Then $f^s + u_n f^s$ for $u_n$ consecutive numbers $s$ (and hence for all large $s$) if and only if a certain finite number of polynomial identities in the variables

Received by the editors July 22, 1974.


Key words and phrases. Boolean ring, recursive sequence, trace, exterior powers, primitive polynomial, exponent.
Let $q = q_1^{t_1} \cdots q_v^{t_v}$ be the prime factorization of $q$. Consider $f : V \rightarrow V$ as a linear map of the $n$-dimensional $\mathbb{Z}_2$-vector space $V$. Put $V_{i} = \ker q_{i}(f)^{t_{i}}$. Then $V = \bigoplus V_{i}$ and the $V_{i}$'s are invariant under $f$. Let $f_{i} : V_{i} \rightarrow V_{i}$ be the restriction of $f$ to $V_{i}$. Then $q_{i}(f)^{t_{i}} = 0$. It is sufficient to show that $u_{n}$ is ultimately a period for $f^{t_{1}}$. If $q_{i} = x$ then $f_{i}$ is nilpotent and we are done.

If $q_{i} \neq x$ we must show that $q_{i}(x)^{u_{n} - 1}$. Assume that $\deg q_{i} = m$. Then $mt_{i} \leq n$, and we have $q_{i}(x)^{m - 1}$. If $2^{r - 1} < n \leq 2^{r}$ then

$$q_{i}(x)^{m - 1} = q_{i}(x)^{m - 1} = x^{2^{r} m - 1} x^{u_{n} - 1}$$

since $2^{r} m | u_{n}$. This proves (a).

(b) Given any $n \times n$ matrix $g = (a_{ij})$ over $\mathbb{Z}_2$, we can find a ring homomorphism $h : B_{2} \rightarrow \mathbb{Z}_2$ such that $h(x_{ij}) = a_{ij}$. Hence if $f^{s+k} = f^{k}$ then we must have $g^{s+k} = g^{k}$.

First let $g$ be the $n \times n$ matrix having minimal polynomial $q = (x+1)^{n}$. Then

$$q = (x + 1)^{n} | (x + 1) 2^{r} = x^{2^{r} - 1}$$

and $q \not| x^{u} - 1$ for $u < 2^{r}$. Hence $\{g^{k}\}_{1}$ has period $2^{r}$ and $2^{r} \not| s$.

Next, if $m < n$, let $g$ be an $n \times n$ matrix having minimal polynomial $q$ where $q$ is a primitive polynomial of degree $m$ having exponent $M_{m}$ (i.e. $q | x^{M_{m}} - 1$, but $q \not| x^{u} - 1$ if $u < M_{m}$). Hence $M_{m} | s$ for all $m \leq n$ and $u_{n} | s$.

By (a) we get $s = u_{n}$.

**Corollary 1.** Let $f$ be an invertible $n \times n$ matrix over $A$. Then $f^{u_{n}} = 1$. The result is best possible.

**Corollary 2.** The exponent of $GL(n, A)$ is $u_{n}$.

**Proof.** By Corollary 1, $f^{u_{n}} = 1$ for all $f$ in $GL(n, A)$. But $A \supset \mathbb{Z}_{2}$ and, by the proof of the second part of the theorem, it follows that $u_{n}$ is the smallest positive integer with this property.

**Corollary 3 (Klöve-Mykkeltveit-Selmer).** Let $\{c_{k}\}_{1}^{\infty}$ be a recursive sequence in $A$ of order $n$, i.e. there exist $a_{1}, a_{2}, \ldots, a_{n}$ in $A$ such that

$$c_{k} = a_{1}c_{k-1} + a_{2}c_{k-2} + \cdots + a_{n}c_{k-n}$$

for $k > n$. Then $u_{n}$ is ultimately a period for $\{c_{k}\}_{1}^{\infty}$.

**Proof.** Let $f$ be the matrix
(0 1 0 \ldots 0 0) \\
(0 0 1 \ldots 0 0) \\
(\ldots \ldots \ldots \ldots \ldots) \\
(0 0 0 \ldots 0 1) \\
(a_n a_{n-1} a_{n-2} \ldots a_2 a_1)

Then \( f(c_1, c_2, \ldots, c_n) = (c_2, c_3, \ldots, c_{n+1}) \) and since \( f^{u_n+k} = f^k \), it follows that \( c_{u_n+k} = c_k \) for all large \( k \).

**Remark.** Corollary 3 was proved by Kløve [3] for \( n \leq 6 \), and for general \( n \) by Mykkeltveit-Selmer [4]. Using the Cayley-Hamilton theorem and considering the recursive sequence of each entry of the powers of \( f \), it is easy to prove Theorem 1 from Corollary 3 (private communication from Kløve). However the first part of Theorem 1 together with Corollary 3 gives a very short proof of Kløve-Mykkeltveit-Selmer's theorem.

Let us now consider the trace sequence \( b_k = \text{Tr}(f^k) \) where \( f \) is an \( n \times n \) matrix. By Theorem 1, \( u_n \) is a period for \( \{b_k\}_{k=1}^\infty \) also, but it is never the period for \( n > 1 \). Actually we have

**Theorem 2.** The period of \( \{\text{Tr}(f^k)\}_{k=1}^\infty \) divides \( v_n \). The result is best possible.

**Proof.** Using the same technique and notation as in the proof of Theorem 1, we get \( \text{Tr}(f^k) = \sum_{i=1}^v \text{Tr}^i(f)^k \) and it suffices to show that the period of \( \{\text{Tr}(f^k)\}_{k=1}^\infty \) divides \( v_n \). Now \( f_i \) has minimal polynomial \( q_i \) and hence \( q_i(f_i) \) is nilpotent. Since \( f_i \) and \( q_i(f_i) \) commute, \( f_i^k q_i(f_i) \) is also nilpotent for all \( k \geq 0 \). It follows that \( \text{Tr}(f_i^k q_i(f_i)) = 0 \). Hence the recursive sequence \( \{\text{Tr}(f_i^k)\}_{k=1}^\infty \) satisfies a recursion formula corresponding to the polynomial \( q_i \). But \( q_i | x^v n - 1 \) unless \( q_i = x \) in which case \( f_i \) is nilpotent. Hence \( \text{Tr}(f_i^k)_{k=1}^\infty \) has period \( v_n \).

To prove that \( v_n \) is best possible we use the same method as in the proof of the second part of Theorem 1. Let \( m \leq n \) and let \( q \) be a primitive polynomial of degree \( m \). If \( g \) is an \( n \times n \) matrix having "characteristic polynomial" \( \det(1 + tg) = q \), then (using the Cayley-Hamilton theorem) we see that \( \{g^k\}_{1}^\infty \) has period \( M_m \). It follows that the reciprocal polynomial of \( q \) is the characteristic polynomial of the sequence \( \{b_k\}_{1}^\infty = \{\text{Tr}g^k\}_{1}^\infty \). But \( q \) and its reciprocal polynomial are irreducible. Hence, either the period of \( \{b_k\}_{1}^\infty \) is \( M_m \), or all \( b_k = 0 \). In the latter case we get a contradiction by the following proposition. Thus \( M_m | v \) for all \( m \leq n \). It follows that \( v_n | s \), and by the first part we get \( s | v_n \) and we are done.

**Proposition 1.** Let \( g \) be any matrix over a Boolean ring. Then \( \text{Tr}g^k = 0 \) for all \( k \) if and only if \( \det(1 + tg) \) is a square.

**Proof.** Put \( b_k = \text{Tr}g^k \) and \( \det(1 + tg) = 1 + a_1 t + a_2 t^2 + \ldots \). We
write down the exponential trace formula (see Almkvist \[1, p. 268\]),
\[a_1 t + a_3 t^3 + a_5 t^5 + \cdots = (1 + a_1 t + a_2 t^2 + \cdots)(b_1 t + b_2 t^2 + \cdots).\]
If all \(b_k = 0\), then \(a_1 = a_3 = a_5 = \cdots = 0\) so
\[\det(1 + tg) = 1 + a_2 t^2 + a_4 t^4 + \cdots = (1 + a_2 t + a_4 t^2 + \cdots)^2.\]

Conversely, if \(\det(1 + tg)\) is a square, then \(a_1 = a_3 = a_5 = \cdots = 0\), so the left-hand side of the exponential trace formula is zero. Then it follows that \(b_k = 0\) for all \(k\).

**Remark.** Since the periods are different, not every recursive sequence in \(A\) is a trace sequence. In fact a trace sequence must satisfy several start conditions (Newton’s formulas, see Almkvist \[1, p. 298\]). In particular we have \(b_{2k} = b_k\) if \(b_k = \text{Tr} f^k\). Hence, \(b_1 = b_3 = b_4 = b_5 = \cdots\) and \(b_3 = b_6 = b_9 = \cdots\). This can be seen as follows (put formally \(t = s^2\)):
\[1 + b_2 t + \cdots = \det(1 + t^{2k}) = \det(1 + (s^k)^2) = \det(1 + s^k)^2 = (1 + b_2 s + \cdots)^2 = 1 + b_2^2 s^2 + \cdots = 1 + b_2 t + \cdots.\]

The trace \(\text{Tr} f\) is just the coefficient of \(t\) in the characteristic polynomial \(\det(1 + tf)\) of \(f\). One can ask what is the period of the sequence of polynomials \(\det(1 + tf^k)\) for \(k = 1\). The result is best possible.

**Theorem 3.** Let \(f\) be an \(n \times n\) matrix. Then \(\nu_n\) is a period for the sequence \(\det(1 + tf^k)\) for \(k = 1, \ldots, \infty\). The result is best possible.

**Proof.** We have
\[\det(1 + tf^k) = 1 + a_{1k} t + a_{2k} t^2 + \cdots + a_{nk} t^n,
\]
where \(a_{pk} = \text{Tr} A^p f^k = \text{Tr}(A^p f^k)\). But \(A^p f : A^p A^n \to A^p A^n\) is a matrix of size \(\binom{n}{p}\) (here \(A^p\) denotes the \(p\)th exterior product, see \[2\]). By Theorem 2 the period \(s\) of \(\nu_n\) divides \(\nu_{n^p}\). On the other hand, by Theorem 1, \(\nu_{n^p}\) has a period dividing \(\nu_n\), and clearly the same thing is true for \(\nu_n\) for all \(p\) with \(1 \leq p < n\). By Theorem 2, \(\nu_{n^p}\) can have period \(\nu_n\), so the result is best possible.

**Conjecture.** Let \(f = (x_{ij})\) be the “free” \(n \times n\) matrix in Theorem 1(b). Then the period of \(\nu_{n^p}\) is \(\nu_n\) for all \(p\) with \(1 \leq p < n\). We collect some evidence for this conjecture.

**Example 1.** Let \(g\) be the \(6 \times 6\) matrix associated with the polynomial \(1 + t^3 + t^5\) of exponent 9.
Then a computation shows that

\[
\det(1 + tg^3) = 1 + t^2 + \cdots, \quad \det(1 + tg^6) = 1 + t + t^3 + \cdots.
\]

It follows that

\[
\text{Tr} A^2 g^3 = 1, \quad \text{Tr} A^2 g^6 = 0.
\]

Hence the sequence \(\{\text{Tr} A^2 g^k\}_{k=1}^{\infty}\) has period 9, and if \(s\) is the period of \(\{\text{Tr} A^2 g^k\}_{k=1}^{\infty}\), then \(9|s\).

Example 2. Let \(g\) be the \(18 \times 18\) matrix associated with the polynomial \(1 + t^9 + t^{18}\) of exponent 27. Then

\[
\det(1 + tg) = 1 + t^9 + t^{18}, \quad \det(1 + tg^{10}) = 1 + t^2 + t^{10} + t^{18}
\]

and

\[
\text{Tr} A^2 g = 0, \quad \text{Tr} A^2 g^{10} = 1.
\]

Hence the period of \(\{\text{Tr} A^2 g^k\}_{k=1}^{\infty}\) is 27, and \(27|s\) if \(s\) is the period of \(\{\text{Tr} A^2 g^k\}_{k=1}^{\infty}\).

REFERENCES


