ZASTOSOWANIA MATEMATYKI
APPLICATIONES MATHEMATICAE
IX, 4 (1968)

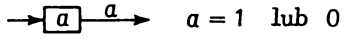
Z. SZWAJA (Poznań)

O ZASTOSOWANIU PEWNYCH WŁASNOŚCI MACIERZY NAD $GF(2)$ DO OPISU AUTOMATÓW LINIOWYCH

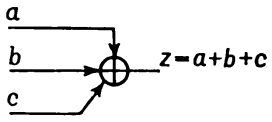
1. Wstęp.

Przez automat liniowy, czyli liniowy układ przełączający, będziemy rozumieć układ złożony z

a) komórek pamięciowych, w których mogą być zapisane wartości 0 lub 1 (rys. 1)



Rys. 1. Schemat komórki pamięciowej



Rys. 2. Sumator mod2 o 3 wejściach

b) sumatorów mod2, tj. elementów realizujących operacje sumowania mod2 (rys. 2):

$$0+0=0$$

$$0+1=1+0=1$$

$$1+1+1+\ldots=\begin{cases}1, & \text{dla } n \text{ nieparzystego},\\ 0, & \text{dla } n \text{ parzystego},\end{cases}$$

c) połączeń między tymi elementami; strzałka oznacza kierunek przechodzenia sygnałów.

Każda komórka pamięciowa ma 1 zacisk wejściowy i 1 zacisk wyjściowy. Przez stan komórki rozumiemy sygnał, jaki jest w niej zapisany; stan ten może więc być równy 0 albo 1. Sygnał określający stan komórki pojawia się na jej zacisku wyjściowym (na jej wyjściu).

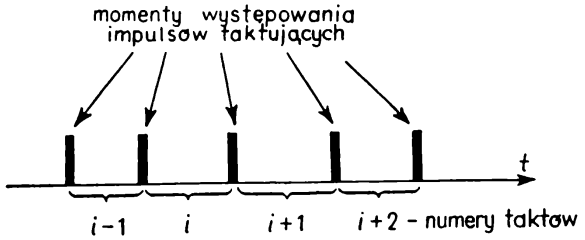
Sumator mod2 ma 2 lub więcej zacisków wejściowych (wejść) i 1 zacisk wyjściowy (wyjście). Do zacisków wejściowych sumatora doprowadza się sygnały z wyjść komórek pamięciowych lub wyjść innych sumatorów.

Przez stan automatu rozumie się określoną kombinację zer i jedynek zapisanych w komórkach, a więc kombinację sygnałów pojawiających

się na zaciskach wyjściowych komórek. Jeśli automat zawiera n komórek, to liczba jego możliwych stanów jest równa 2^n.

Zmiana stanu automatu następuje w wyniku przykładania tzw. impulsów taktujących; wtedy w komórkach zostają zapisane sygnały, które występowały na ich wejściach tuż przed przyłożeniem impulsów taktujących.

Pracę automatu liniowego można opisać za pomocą 2 układów równań liniowych [9] określających sygnały wyjściowe automatu w takcie i w zależności od sygnałów wejściowych i od stanu automatu w takcie i oraz stan automatu w takcie $i+1$ w zależności od wartości sygnałów wejściowych i od stanu automatu w takcie i; przez takty rozumie się tu przedziały czasu przedstawione orientacyjnie na rys. 3



Rys. 3. Schematyczne przedstawienie taktów

Jeśli sygnały wejściowe są równe zeru i jeśli interesuje nas tylko stan automatu, to wtedy mamy do czynienia z tzw. pracą autonomiczną, którą można opisać za pomocą jednego układu równań liniowych [4]

$$\boldsymbol{v}_{i+1} = \boldsymbol{v}_i T,$$

gdzie $\boldsymbol{v}_i$ — wektor o r składowych z $GF(2)$(1) charakteryzujący stan r komórek w takcie i, czyli wektor stanu automatu w takcie i, $\boldsymbol{v}_{i+1}$ — wektor stanu automatu w takcie $i+1$, T — macierz stopnia r o elementach z $GF(2)$

$$T = \begin{bmatrix} t_{11} & t_{12} & \dots & t_{1r} \\ t_{21} & t_{22} & \dots & t_{2r} \\ \dots & \dots & \dots & \dots \\ r_{ri} & t_{r2} & \dots & t_{rr} \end{bmatrix},$$

(1) $GF(2)$ — ciało Galois złożone z 2 elementów: 0 i 1, czyli inaczej zbiór złożony z zera i jedynki z operacją dodawania i mnożenia mod 2:

$$1+0 = 0+1 = 1$$
$$1+1 = 0+0 = 0$$
$$1 \cdot 1 = 1$$
$$1 \cdot 0 = 0 \cdot 1 = 0 \cdot 0 = 0$$

$t_{mn} = 1$ oznacza, że wyjście m-tej komórki połączone jest z wejściem n-tej komórki, czyli, że stan m-tej komórki ma wpływ na stan n-tej komórki, $t_{mn} = 0$ oznacza brak połączenia wyjścia m-tej komórki z wejściem n-tej komórki.

W dalszym ciągu interesować nas będzie tylko praca autonomiczna automatu liniowego; zadaniem niniejszych rozważań jest podanie sposobu na wyznaczanie liczby taktów, po której automat wraca do stanu początkowego. Zostanie to omówione w oparciu o znajomość wielomianu stopnia r nad $GF(2)$, z którym macierz T jest stowarzyszona. Zagadnienie to, które można rozpatrywać w oderwaniu od automatów, można postawić następująco:

a. Dla macierzy kwadratowej T stopnia r nad $GF(2)$ należy znaleźć długość okresu n, tj. taką najmniejszą liczbę n, że zachodzi

$$T^n = I.$$

b. Niech v oznacza ciąg nad $GF(2)$ o długości r złożony ze współczynników wielomianu $v(x)$ stopnia nie większego niż $r-1$; znając związek $v(x)$ z wielomianem stopnia r, z którym stowarzyszona jest macierz T, należy znaleźć najmniejszą liczbę $l \leqslant n$ taką, że

$$vT^l = v.$$

c. Należy znaleźć liczbę ciągów, dla których ta zależność zachodzi.

W trakcie początkowych rozważań pokazuje się, że macierz T stopnia m stowarzyszoną z wielomianem pierwotnym stopnia m można rozważać jako element pierwotny w $GF(2^m)$. Jeżeli 2^m-1 jest liczbą pierwszą, to wtedy każda z potęg takiej macierzy T (z wyjątkiem T^0) generuje grupę multiplikatywną $GF(2^m)$.

Wszystkie te właściwości macierzy mają prostą interpretację fizyczną — stanowią one modele matematyczne odpowiednich automatów liniowych.

Podstawą rozważań jest fakt, że każda macierz ma swój wielomian charakterystyczny i minimalny oraz że do każdego wielomianu nad $GF(2)$

$$f(x) = a_0 + a_1 x + \ldots + a_{m-1} x^{m-1} + a_m x^m$$

można określić macierz stowarzyszoną [3]

$$\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_0 & a_1 & a_2 & \ldots & a_{m-1} \end{bmatrix}.$$

Macierz ta zawiera w ostatnim wierszu elementy $a_0, a_1, \ldots, a_{m-1}$, jedynki nad główną przekątną, a poza tym same zera.

2. Automaty opisywane przez macierze pierwotne i ich potęgi.

2.1. Właściwości wielomianów pierwotnych i stowarzyszonych z nimi macierzy. Dla potrzeb opisu automatów liniowych celowy jest podział wielomianów na rozkładalne i nierozkładalne nad $GF(2)$. Wśród tych ostatnich wyróżnia się jeszcze tzw. wielomiany pierwotne, charakteryzujące się tym, że rząd pierwiastków takiego wielomianu jest równy 2^m-1, gdzie m jest stopniem wielomianu nad $GF(2)$. Inaczej mówiąc, pierwiastek wielomianu pierwotnego nad $GF(2)$ stopnia m jest generatorem grupy multyplikatywnej $GF(2^m)$ [2]. Ponieważ macierz stowarzyszona z wielomianem stopnia m jest jego pierwiastkiem, więc jeśli wielomian jest pierwotny, to stowarzyszoną z nim macierz T można traktować jako pewien sposób przedstawienia elementu pierwotnego w $GF(2^m)$. Oznacza to, że potęgi macierzy T będą niezerowymi elementami $GF(2^m)$ i że $n = 2^m-1$ jest najmniejszą liczbą całkowitą taką, że $T^n = I$. Tak więc dowolny ciąg zero-jedynkowy o długości m pomnożony przez $T^n = T^{2m-1}$ daje ten sam ciąg i nie ma potęgi mniejszej niż $n = 2^m-1$, do której podniesiona macierz T spełniałaby ten sam warunek. Znaczy to, że dowolny ciąg o długości m pomnożony przez potęgę macierzy T mniejszą niż $n = 2^m-1$ daje zawsze inny ciąg. Ciągi te możemy również traktować jako elementy $GF(2^m)$. Zależności między poszczególnymi elementami $GF(2^m)$ są określone przez dany wielomian; zilustrowano to poniżej na kilku przykładach.

Jeśli macierz T jest pierwiastkiem wielomianu pierwotnego stopnia m, to jego pierwiastkami są również $T^2, (T^2)^2, \ldots, (T^2)^{m-1}$. Jeśli idzie o inne potęgi macierzy T (z wyjątkiem $T^0 = I$), to w zależności od tego, czy 2^m-1 jest liczbą pierwszą czy nie, mogą one wszystkie albo tylko część z nich generować grupę multiplikatywną $GF(2^m)$. W pierwszym przypadku każda z potęg macierzy T ma okres o długości $n = 2^m-1$ tj. 2^m-1 jest najmniejszą liczbą n taką, że $T^n = T^{2^m-1} = I$. W drugim przypadku dotyczy to tylko niektórych potęg T.

Przykład 1. Macierz stowarzyszona z wielomianem pierwotnym $f(x) = 1+x+x^3$ jest równa

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

W myśl tego, co wyżej powiedziano, niezerowymi elementami $GF(2^3)$ są: $T^0 = I$, T, T^2, T^3, T^4, T^5 i T^6 ($T^7 = I$). Zbiór ten, tworzący grupę multyplikatywną $GF(2^3)$, może być również generowany przez $T^2[(T^2)^0 = I$, $(T^2)^1 = T^2$, $(T^2)^2 = T^4$, $(T^2)^3 = T^6$, $(T^2)^4 = T^8 = T$, $(T^2)^5 = T^{10} = T^3$, $(T^2)^6 = T^{12} = T^5]$ albo przez T^4.

Wielomian charakterystyczny macierzy T, T^2 i T^4 jest równy x^3+x+1. Pozostałe elementy $GF(2^3)$ oprócz elementów neutralnych, tj. oprócz 0 i 1, mogą również generować wszystkie niezerowe elementy $GF(2^3)$. Generatorami $GF(2^3)$ mogą więc być także T^3, T^5 i T^6. Należy jednak mieć na uwadze, że wielomianem charakterystycznym tych macierzy jest x^3+x^2+1, a więc słuszna jest np. zależność $(T^5)^3+(T^5)^2+I=0$.

Przykład 2. Macierzą stowarzyszoną z wielomianem $f(x)=1+x+x^4$ jest

$$T=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0\end{bmatrix}.$$

Możemy ją traktować jako element pierwotny $GF(2^4)$, a więc wszystkie niezerowe elementy $GF(2^4)$ można wyrazić w postaci potęg T lub w postaci liniowych kombinacji macierzy I, T, T^2 i T^3:

$$\begin{aligned}
T^0&=I & T^8&=I+T^2\\
T^1&=T & T^9&=T+T^3\\
T^2&=T^2 & T^{10}&=I+T+T^2\\
T^3&=T^3 & T^{11}&=T+T^2+T^3\\
T^4&=I+T & T^{12}&=I+T+T^2+T^3\\
T^5&=T+T^2 & T^{13}&=I+T^2+T^3\\
T^6&=T^2+T^3 & T^{14}&=I+T^3\\
T^7&=I+T+T^3 & T^{15}&=I
\end{aligned}$$

Poszczególne potęgi macierzy można znaleźć z tablicy 1.

TABLICA 1. Potęgi macierzy T stowarzyszonej z wielomianem x^4+x+1

$$\left.\begin{matrix}0\,1\,0\,0\\0\,0\,1\,0\\0\,0\,0\,1\\1\,1\,0\,0\end{matrix}\right\}T\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^2\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^3\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^4$$

$$\left.\begin{matrix}0\,1\,1\,0\\0\,0\,1\,1\\1\,1\,0\,1\\1\,0\,1\,0\end{matrix}\right\}T^5\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^6\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^7\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^8$$

$$\left.\begin{matrix}0\,1\,0\,1\\1\,1\,1\,0\\0\,1\,1\,1\\1\,1\,1\,1\end{matrix}\right\}T^9\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^{10}\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^{11}\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^{12}$$

$$\left.\begin{matrix}1\,0\,1\,1\\1\,0\,0\,1\\1\,0\,0\,0\\0\,1\,0\,0\end{matrix}\right\}T^{13}\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^{14}\quad\left.\begin{matrix}\\\\\\\end{matrix}\right\}T^{15}=I$$

$$0\,0\,1\,0$$

$$0\,0\,0\,1$$

Tak np. T^7 jest równa

$$T^7 = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

Macierz T jest pierwiastkiem wielomianu $g(x) = 1+x+x^4$. Pierwiastkami są również macierze: T^2, T^4 i T^8. Innymi słowy, macierze T, T^2, T^4 i T^8 mają ten sam wielomian charakterystyczny x^4+x+1, są więc podobne.

Wielomianem charakterystycznym i minimalnym macierzy T^3 i tym samym macierzy $(T^3)^2 = T^6$, $(T^3)^4 = T^{12}$ i $(T^3)^8 = T^9$, jest $x^4+x^3+x^2+x+1$. Okres macierzy T^3 jest równy 5, bo $(T^3)^5 = I$; oznacza to, że nie możemy wyrazić wszystkich niezerowych elementów $GF(2^4)$ w postaci potęg macierzy T^3. Dowolny ciąg zero-jedynkowy o długości 4 pomnożony przez potęgi T^3 daje łącznie tylko 5 różnych ciągów. Muszą więc istnieć 3 rozłączne zbiory takich ciągów, które w sumie dają 15 niezerowych ciągów.

Wielomianem charakterystycznym i minimalnym macierzy T^7 oraz $(T^7)^2 = T^{14}$, $(T^{14})^2 = T^{28} = T^{13}$ i $(T^{13})^2 = T^{26} = T^{11}$ jest x^4+x^3+1. Natomiast wielomianem minimalnym macierzy

$$T^5 = T+T^2 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

jest x^2+x+1; zachodzi więc $(T^5)^2+T^5+I = 0$. Wielomian ten znajdujemy ze wzoru [5]

$$m(x) = \frac{D_n(x)}{D_{n-1}(x)},$$

gdzie $D_n(x)$ jest wielomianem charakterystycznym danej macierzy, a $D_{n-1}(x)$ jest największym wspólnym dzielnikiem minorów stopnia $n-1$ macierzy $Ix+T^5$, tj. macierzy charakterystycznej dla macierzy T^5. W naszym przypadku $D_n(x) = x^4+x^2+1$, $D_{n-1}(x) = x^2+x+1$.

Obliczanie $m(x)$ jest w zasadzie bardzo proste, ale przy macierzach wyższego stopnia wymaga dużej liczby operacji. Dlatego wygodniej jest korzystać z tabel Marsha [9], które podają dla poszczególnych elementów $GF(2^m)$ wielomiany minimalne. Dla ilustracji, w oparciu o wspomniane tabele, podano wykaz wielomianów minimalnych dla elementów $GF(2^6)$. Założono, że generatorem grupy multyplikatywnej tego ciała jest macierz T stowarzyszona z wielomianem x^6+x+1. Podano również okresy

macierzy T^i, tj. najniższe ich potęgi e takie, że $(T^i)^e = I$. Znajduje się je ze wzoru [9]

$$e = \frac{2^m - 1}{NWD(2^m - 1, i)}.$$

TABLICA 2. Wykaz wielomianów minimalnych dla elementów $GF(2^6)$

Potęgi T^i	Wielomian minimalny $m(x)$	e
1(2, 4, 8, 16, 32)	x^6+x+1	63
3(6, 12, 24, 33, 48)	$x^6+x^4+x^2+x+1$	21
5(10, 17, 20, 34, 40)	$x^6+x^5+x^2+x+1$	63
7(14, 28, 35, 49, 56)	x^6+x^3+1	9
9(18, 36)	x^3+x^2+1	7
11(22, 25, 37, 44, 50)	$x^6+x^5+x^3+x^2+1$	63
13(19, 26, 38, 41, 52)	$x^6+x^4+x^3+x+1$	63
21(42)	x^2+x+1	3
23(29, 43, 46, 53, 58)	$x^6+x^5+x^4+x^2+1$	63
27(45, 54)	x^3+x+1	7
31(47, 55, 59, 61, 62)	x^6+x^5+1	63

Okresy macierzy T^i w $GF(2^4)$ są następujące:

i	okres e	
1	15	bo $T^{15} = I$
3	5	bo $(T^3)^5 = I$
5	3	bo $(T^5)^3 = I$
7	15	bo $(T^7)^{15} = I$

Tak więc dowolny ciąg 4-pozycyjny pomnożony przez $(T^5)^3$ daje ten sam ciąg:

$$1000\cdot(T^5)^0 = 1000 \quad 1100\cdot(T^5)^0 = 1100$$
$$1000\cdot(T^5)^1 = 0110 \quad 1100\cdot(T^5)^1 = 0101$$
$$1000\cdot(T^5)^2 = 1110 \quad 1100\cdot(T^5)^2 = 1001$$
$$1000\cdot(T^5)^3 = 1000 \quad 1100\cdot(T^5)^3 = 1100$$
itd.

Należy zwrócić uwagę na to, że macierz

$$T_5 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

stowarzyszona z wielomianem charakterystycznym macierzy T^5 nie jest podobna do macierzy T^5, gdyż wielomian minimalny macierzy T_5 jest równy jej wielomianowi charakterystycznemu, tj. równy x^4+x^2+1, a nie x^2+x+1 jak w przypadku macierzy T^5.

Okres macierzy T_5 jest równy 6, bo $(x^4+x^2+1)|(x^6+1)$. Dowolny ciąg o długości 4 pomnożony przez T_5^6 daje taki sam ciąg. Ponieważ wszystkich niezerowych ciągów nad $GF(2)$ o długości 4 jest 15, musi więc istnieć jakiś ciąg, który pomnożony przez T_5^3 daje taki sam ciąg; jest nim ciąg podzielny przez x^2+x+1 [2].

Macierz T^5 jest natomiast podobna do macierzy quasi-diagonalnej

$$T_q = \begin{bmatrix} 0 & 1 & & \\ 1 & 1 & & 0 \\ & & \ddots & \\ & 0 & & \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix} \end{bmatrix},$$

której wielomianem charakterystycznym jest x^4+x^2+I, a minimalnym x^2+x+I. Tak więc dowolny 4-pozycyjny ciąg pomnożony przez T_q^3 daje taki sam ciąg:

$$\begin{aligned}
&1\,0\,0\,0\cdot(T_q)^0 = 1\,0\,0\,0 \qquad 0\,1\,0\,1\cdot(T_q)^0 = 0\,1\,0\,1\\
&1\,0\,0\,0\cdot(T_q)^1 = 0\,1\,0\,0 \qquad 0\,1\,0\,1\cdot(T_q)^1 = 1\,1\,1\,1\\
&1\,0\,0\,0\cdot(T_q)^2 = 1\,1\,0\,0 \qquad 0\,1\,0\,1\cdot(T_q)^2 = 1\,0\,1\,0\\
&1\,0\,0\,0\cdot(T_q)^3 = 1\,0\,0\,0 \qquad 0\,1\,0\,1\cdot(T_q)^3 = 0\,1\,0\,1
\end{aligned}$$

2.2. Interpretacja fizyczna. Interpretacja fizyczna tych właściwości macierzy w ich zastosowaniu do automatów liniowych jest prosta:

a) automat liniowy opisywany przez wielomian pierwotny lub stowarzyszoną z nim macierz stopnia m ma 2^m-1 niezerowych stanów niezależnie od stanu początkowego;

b) jeśli automat jest opisywany przez macierz, która jest pewną potęgą i macierzy T stowarzyszonej z wielomianem pierwotnym, to 2^m-1 niezerowych stanów dzieli się na k cykli każdy o długości e, która jest rzędem pierwiastka wielomianu minimalnego macierzy T^i. Dotyczy to zarówno przypadku, kiedy wielomian charakterystyczny macierzy T^i jest jej wielomianem minimalnym, jak i przypadku, kiedy wielomian charakterystyczny jest wielokrotnością wielomianu minimalnego.

Macierz stowarzyszona z wielomianem charakterystycznym danej macierzy nie jest w ogólnym przypadku do niej podobna i tym samym automaty opisywane przez te macierze zachowują się inaczej.

Przykłady. Podano schematy i wykaz niezerowych stanów automatów opisywanych przez:

---

[2] Każdy ciąg zero-jedynkowy $v = (a_0, a_1, \ldots, a_{m-1})$ można nazwać wielomianem nad $GF(2)$ (np. [5], str. 168-175) i zapisać go w postaci $v(x) = a_0+a_1x+\ldots+a_{m-1}x^{m-1}$. Wyrażenie „ciąg v jest podzielny przez wielomian $h(x)$" mówi, że zachodzi $v(x) = q(x)h(x)$. Tak np. jeśli $h(x) = x^2+x+1$ i $v = 1001$, to $v(x) = 1+x^3 = (x+1)(x^2+x+1)$.

1. Macierz T stowarzyszoną z wielomianem pierwotnym x^4+x+1.
2. Macierz T^3.
3. Macierz T_3 stowarzyszoną z wielomianem charakterystycznym macierzy T^3.
4. Macierz T^5.
5. Macierz quasi-diagonalną T_q podobną do macierzy T^5.
6. Macierz T_5 stowarzyszoną z wielomianem charakterystycznym macierzy T^5.

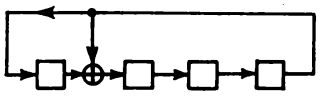
Wielomiany charakterystyczne i minimalne tych macierzy oraz długości ich okresów zebrane są w tablicy 3.

TABLICA 3. Wykaz właściwości macierzy z przykładów 1-6

Przykład	Macierz	Wielomian		Długość okresu	Schemat
		charakterystyczny	minimalny		
1	T	x^4+x+1	x^4+x+1	15	rys. 4
2	T^3	$x^4+x^3+x^2+x+1$	$x^4+x^3+x^2+x+1$	5	rys. 5
3	T_3	$x^4+x^3+x^2+x+1$	$x^4+x^3+x^2+x+1$	5	rys. 6
4	T^5	x^4+x^2+1	x^2+x+1	3	rys. 7
T	T_q	x^4+x^2+1	x^2+x+1	3	rys. 8
6	T_5	x^4+x^2+1	x^4+x^2+1	6	rys. 9

1. Macierz T stowarzyszona z wielomianem pierwotnym x^4+x+1

$$T = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}.$$

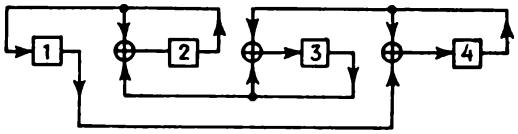


1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1
1	1	0	0
0	1	1	0
0	0	1	1
1	1	0	1
1	0	1	0
0	1	0	1
1	1	1	0
0	1	1	1
1	1	1	1
1	0	1	1
1	0	0	1

Rys. 4. Schemat i stany niezerowe automatu opisywanego przez macierz T

2. Macierz T^3

$$T^3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

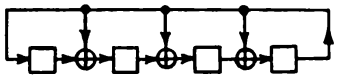


1	0	0	0
0	0	0	1
0	0	1	1
0	1	0	1
1	1	1	1
.	.	.	.
1	1	0	0
1	1	0	1
1	1	1	0
1	0	1	1
0	1	0	0
.	.	.	.
1	0	1	0
0	1	1	1
1	0	0	1
0	0	1	0
0	1	1	0
.	.	.	.

Rys. 5. Schemat i stany niezerowe automatu opisywanego przez macierz T^3

3. Macierz T_3 stowarzyszona z wielomianem charakterystycznym macierzy T^3

$$T_3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

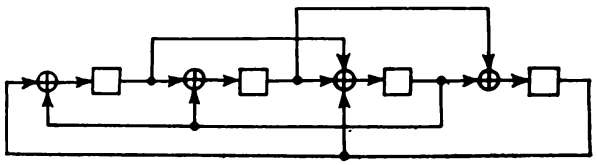


1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1
1	1	1	1
.	.	.	.
1	1	0	0
0	1	1	0
0	0	1	1
1	1	1	0
0	1	1	1
.	.	.	.
1	0	1	0
0	1	0	1
1	1	0	1
1	0	0	1
1	0	1	1
.	.	.	.

Rys. 6. Schemat i stany niezerowe automatu opisywanego przez macierz T_3

4. Macierz T^5

$$T^5 = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

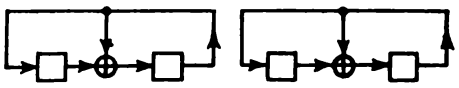


1	0	0	0
0	1	1	0
1	1	1	0
0	1	0	0
0	0	1	1
0	1	1	1
0	0	1	0
1	1	0	1
1	1	1	1
0	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
0	1	0	1
1	0	0	1

Rys. 7. Schemat i stany niezerowe automatu opisywanego przez macierz T^5

5. Macierz quasi-diagonalna T_q podobna do macierzy (T^5)

$$T_q = \left[\begin{array}{cc:c} 0 & 1 & \\ 1 & 1 & 0 \\ \hdashline & & 0 \; 1 \\ 0 & & 1 \; 1 \end{array}\right]$$

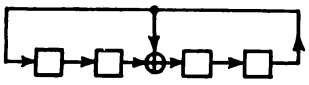


1	0	0	0
0	1	0	0
1	1	0	0
0	0	1	0
0	0	0	1
0	0	1	1
1	0	1	0
0	1	0	1
1	1	1	1
1	0	0	1
0	1	1	1
1	1	1	0
0	1	0	1
1	1	1	1
1	0	1	0

Rys. 8. Schemat i stany niezerowe automatu opisywanego przez macierz quasi-diagonalną T_q

6. Macierz stowarzyszona z wielomianem charakterystycznym T^5

$$T_5 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$



1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1
1	0	1	0
0	1	0	1
.	.	.	.
1	1	0	0
0	1	1	0
0	0	1	1
1	0	1	1
1	1	1	1
1	1	0	1
.	.	.	.
1	0	0	1
1	1	1	0
0	1	1	1
.	.	.	.

Rys. 9. Schemat i stany niezerowe automatu opisywanego przez macierz T_5

3. Automaty opisywane przez wielomiany typu $f(x) = [\varphi(x)]^m$.

3.1. Przypadek $f(x) = (x+1)^m$. Okres macierzy T stopnia m, której wielomian charakterystyczny i minimalny wynosi $(x+1)^m$, jest równy 2^k, gdzie k jest takie, że

$$2^{k-1} < m \leqslant 2^k.$$

Dla $m = 1\text{-}64$ długości okresów podane są w tablicy 4.

TABLICA 4. Długości okresów macierzy stowarzyszonej z $f(x) = (1+x)^m$

m	1	2	3...4	5...8	9...16	17...32	33...64
Długość okresu	2^0	2	2^2	2^3	2^4	2^5	2^6

Znalezienie długości okresu macierzy stowarzyszonej z wielomianem $f(x)$ nad $GF(2)$ sprowadza się do określenia najmniejszej liczby całkowitej n takiej, że $f(x)|(x^n+1)$. W tym konkretnym przypadku $f(x) = (x+1)^m$

musi być dzielnikiem $(x+1)^n = x^n+1$; żeby ta ostatnia zależność zachodziła, n musi być potęgą liczby 2 (p. np. [3], str. 405), a to prowadzi do wzoru jak wyżej.

Istnieją ciągi v o długości m takie, że

$$v \cdot T^{2^{k_1}} = v, \qquad k_1 \leqslant k.$$

Obowiązującą tu prawidłowość można ująć następująco: jeśli ciąg v wyrażony w postaci wielomianu jest podzielny przez $(x+1)^l$ (por. odsyłacz na str. 398), to wtedy k_1 określa się ze wzoru

$$2^{k_1-1} < (m-l) \leqslant 2^{k_1}.$$

Przykład. Niech $f(x) = (x+1)^5 = x^5+x^4+x+1$, $m = 5$, wobec czego okres macierzy stowarzyszonej z $f(x)$ jest równy $8 = 2^3$, bo

$$2^2 < 5 < 2^3.$$

Jeżeli ciąg v wyrażony w postaci wielomianu jest podzielny przez $x+1$, a niepodzielny przez $(x+1)^l$, $l > 1$, to wtedy

$$v \cdot T^4 = v,$$

bo

$$2^{2-1} < 5-1 = 2^2.$$

Podobnie jeśli ciąg v jest podzielny przez $(1+x)^4$, to

$$v \cdot T^1 = v, \qquad 2^{-1} < 5-4 = 2^0 = 1.$$

W oparciu o fakt, że dla macierzy stopnia m z 2^m-1 niezerowych ciągów istnieje

2^{m-1} ciągów podzielnych tylko przez $(x+1)^0 = 1$

2^{m-2} ciągów podzielnych tylko przez $(x+1)^1$

2^{m-3} ciągów podzielnych tylko przez $(x+1)^2$

. . . . . .

2^{m-m} ciągów podzielnych tylko przez $(x+1)^{m-1}$

można określić długości cykli i ich liczbę dla poszczególnych wartości m. Zebrano to w tablicy 5.

TABLICA 5. Liczba okresów dla przypadku $f(x) = (1+x)^m$

Długość okresu → / m ↓	1	2	4	8	16
1	1				
2	1	1			
3	1	1	1		
4	1	1	3		
5	1	1	3	$2 = 2\cdot 1$	
6	1	1	3	$6 = 2\cdot 3$	
7	1	1	3	$14 = 2\cdot 7$	
8	1	1	3	$30 = 2\cdot 15$	
9	1	1	3	30	$16 = 16\cdot 1$
10	1	1	3	30	$48 = 16\cdot 3$
11	1	1	3	30	$112 = 16\cdot 7$
. . . . .	. . . . .	. . . . .	. . . . .	. . . . .	. . . . .
16	1	1	3	30	$4080 = 16\cdot 255$

Tak np. dla macierzy stopnia 9, stowarzyszonej z wielomianem $(x+1)^9 = x^9+x^8+x+1$, z $2^9-1 = 511$ niezerowych ciągów jest 2^8 ciągów podzielnych tylko przez $(x+1)^0 = 1$. Ponieważ

$$2^3 < (9-0) < 2^4 = 16,$$

więc ciągi te tworzą cykle o długości 16. Dalej, ponieważ $2^8 = 256 = 16\cdot 16$, zatem liczba cykli jest równa 16. Z pozostałych 255 ciągów jest

$2^7 = 128$ ciągów podzielnych przez $(x+1)$,
$2^6 = 64$ ciągów podzielnych przez $(x+1)^2$,
$2^5 = 32$ ciągów podzielnych przez $(x+1)^3$,
$2^4 = 16$ ciągów podzielnych przez $(x+1)^4$.

Ponieważ

$$2^2 < (9-1) = 8, \quad 2^2 < (9-2) < 8,$$

$$2^2 < (9-3) < 8 \quad 2^2 < (9-4) < 8,$$

więc (por. str. 402) wszystkie te ciągi w liczbie $128+64+32+16 = 240$ tworzą cykle o długości 8. Ich liczba wynosi $\frac{240}{8} = 30$.

Z pozostałych $2^4-1 = 15$ ciągów jest $2^3 = 8$ ciągów podzielnych przez $(x+1)^5$, $2^2 = 4$ ciągi podzielne przez $(x+1)^6$. Ponieważ

$$2 < (9-5) = 4, \quad 2 < (9-6) < 4,$$

więc te 12 ciągów tworzą cykle o długości 4; ich liczba jest równa $\frac{12}{4} = 3$.

Z pozostałych 3 ciągów są 2 ciągi podzielne przez $(x+1)^7$ i 1 ciąg podzielny przez $(x+1)^8$; daje to 1 cykl o długości 2, bo

$$2^0 < (9-7) = 2^1 = 2$$

(są to ciągi 1 1 1 1 1 1 1 1 0 i 0 1 1 1 1 1 1 1 1), oraz 1 cykl o długości 1, bo

$$2^{-1} < (9-8) = 2^0 = 1$$

(jest to ciąg 1 0 0 0 0 0 0 0 1).

3.2. Przypadek $f(x) = [\varphi(x)]^m$; $\varphi(x)$ = wielomian pierwotny stopnia $\geqslant 2$. Długość okresów macierzy stowarzyszonych z $f(x) = [\varphi(x)]^m$, gdzie $\varphi(x)$ jest wielomianem pierwotnym stopnia $j = 2, 3, \ldots$, jest równa

$$(2^j-1)2^k,$$

gdzie k spełnia warunek jak dla $j = 1$:

$$2^{k-1} < m \leqslant 2^k.$$

Dla wartości j = 1-6 i m = 1-64 wartości długości okresów macierzy podano w tablicy 6.

TABLICA 6. Długości okresów macierzy stowarzyszonych z wielomianami $f(x) = [\varphi(x)]^m$; $\varphi(x)$ = wielomian pierwotny stopnia j

j \ m		1	2	3-4	5-8	9-16	17-32	33-64
1	1							
2	3							
3	7							
4	15	$\cdot 2^0$	$\cdot 2^1$	$\cdot 2^2$	$\cdot 2^3$	$\cdot 2^4$	$\cdot 2^5$	$\cdot 2^6$
5	31							
6	63							

Tak więc np. długością okresu macierzy stowarzyszonej z wielomianami $(x^2+x+1)^{11}$ jest $(2^2-1)\cdot 2^4 = 48$, a macierzy stowarzyszonej z $(x^6+x^5+1)^7$ jest $(2^6-1)\cdot 2^3 = 63\cdot 8 = 504$.

Rozpatrzymy szczegółowo przypadek $\varphi(x) = x^2+x+1$. Wielomianem typu x^n+1 o najmniejszej wartości n podzielnym przez x^2+x+1 jest x^3+1, czyli

$$(x^2+x+1) \mid (x^3+1).$$

Wobec tego zachodzi również

$$(x^2+x+1)^2 \mid (x^3+1)^2 = x^6+1$$

oraz

$$(x^2+x+1)^3 \mid (x^3+1)^3,$$

ale ponieważ $(x^3+1)^3 \neq x^9+1$, więc rząd macierzy stowarzyszonej z $(x^2+x+1)^3$ będzie równy 12, bo $(x^3+1)^3 | (x^3+1)^4 = x^{12}+1$.

Rozumując w podobny sposób, znajdujemy wzór na długość okresu jak wyżej.

Wartość potęgi l w wyrażeniu

$$v \cdot T^l = v,$$

gdzie v jest ciągiem nad $GF(2)$ o długości $j \cdot m$ podzielnym przez $[\varphi(x)]^b$, a T jest macierzą stowarzyszoną z $[\varphi(x)]^m$, jest równa

$$l = (2^j - 1)2^e,$$

gdzie $e = ld(m-b)$, jeśli $m-b$ jest potęgą liczby 2, $e = E[1+ld(m-b)]$, jeśli $m-b$ nie jest potęgą 2. Innymi słowy e spełnia warunek

$$2^{e-1} < (m-b) \leqslant 2^e.$$

Tak więc np. jeśli T jest macierzą stowarzyszoną z wielomianem $(x^2+x+1)^6$, to będzie dla

$$v_1 = 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0 \quad - \quad v_1 T^{24} = v_1,$$

a dla

$$v_2 = 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0 \quad - \quad v_2 T^{12} = v_2,$$

bo v_1 jest podzielny tylko przez $(x^2+x+1)^1$, a więc jest

$$2^2 < (6-1) = 5 < 2^3$$

i tym samym długość cyklu jest równa $3 \cdot 2^3 = 24$, a v_2 jest podzielny przez $(x^2+x+1)^2$ i długość cyklu jest $3 \cdot 2^2 = 12$, bo

$$2^1 < (6-2) = 4 = 2^2.$$

Liczba cykli o długości 3, 6, 12, 24 dla potęg $m = 1\text{-}8$ wielomianu x^2+x+1 podana jest w tablicy 7.

TABLICA 7. Liczba okresów o długości 3, 6, 12, 24 dla przypadku $f(x) = (x^2+x+1)^m$

$m\downarrow$ \ Długość cyklu $\rightarrow$	3	6	12	24
1	1			
2	1	2		
3	1	2	4	
4	1	2	20	
5	1	2	20	32
6	1	2	20	160
7	1	2	20	672
8	1	2	20	2720

Sposób znajdowania tych liczb pokażemy w oparciu o macierz stowarzyszoną z $(x^2+x+1)^3$. Obliczymy ile 6-elementowych ciągów nad $GF(2)$ jest podzielnych przez $(x^2+x+1)^2$, ile przez $(x^2+x+1)^1$ i ile przez $(x^2+x+1)^0 = 1$. Ponieważ $(x^2+x+1)^2 = x^4+x^2+1$, więc zarówno ciąg $1+x^2+x^4$, czyli 1 0 1 0 1 0, jak i ciąg $(1+x^2+x^4)x$, czyli 0 1 0 1 0 1, oraz ich liniowa kombinacja, czyli 1 1 1 1 1 1, są podzielne przez $(x^2+x+1)^2$. Łączna liczba takich ciągów jest równa 3. Można powiedzieć, że stanowią one podprzestrzeń wektorową, której wektorami bazy są ciągi

$$1\ 0\ 1\ 0\ 1\ 0 \ — \ (1+x^2+x^4), \quad 0\ 1\ 0\ 1\ 0\ 1 \ — \ (x+x^3+x^5).$$

Podobnie wektorami bazy podprzestrzeni wektorów podzielnych przez x^2+x+1 są następujące ciągi:

$$1\ 1\ 1\ 0\ 0\ 0\ (1+x+x^2), \quad 0\ 1\ 1\ 1\ 0\ 0\ (1+x+x^2)x,$$

$$0\ 0\ 1\ 1\ 1\ 0\ (1+x+x^2)x^2, \quad 0\ 0\ 0\ 1\ 1\ 1\ (1+x+x^2)x^3.$$

Ciągi te wraz z ich liniowymi kombinacjami tworzą podprzestrzeń złożoną z 15 niezerowych wektorów. Tak więc istnieje 15 niezerowych wektorów (ciągów) podzielnych przez x^2+x+1. Rzecz jasna, że 3 wektory podzielne przez $(x^2+x+1)^2$ są podzielne również przez x^2+x+1. Tak więc wektorów podzielnych tylko przez x^2+x+1 (a nie przez $(x^2+x+1)^2$) jest 12. Ponieważ długość cyklu jest równa 6, więc liczba cykli jest równa 2.

Liczba ciągów podzielnych przez 1 jest $2^6-1 = 63$. Odliczając od tego ciągi podzielne przez x^2+x+1, otrzymamy $63-15 = 48$ ciągów podzielnych przez 1. Wobec długości cyklu równej 12 (bo $T^{12} = I$) otrzymuje się ich liczbę 4.

W podobny sposób znajdujemy liczby okresów dla macierzy stowarzyszonych z potęgami wielomianów pierwotnych stopnia trzeciego, czwartego, piątego, ...

3.3. Przypadek $f(x) = [\varphi(x)]^m$; $\varphi(x)$ = wielomian nierozkładalny, niepierwotny. Jeśli idzie o potęgi wielomianów nierozkładalnych, niepierwotnych stopnia j, to — zważywszy, że liczba 2^j-1 jest złożona (por. wzór na e, str. 397) — długości okresów są dzielnikami długości cykli odpowiadających wielomianom pierwotnym tego samego stopnia. Tak np. dla przypadku macierzy stowarzyszonej z kwadratem wielomianu pierwotnego szóstego stopnia, $j = 6$, $m = 2$; $f(x) = (x^6+x+1)^2$, mamy 1 okres o długości 63 i $\dfrac{(2^{12}-1)-63}{63\cdot 2^1} = 32$ okresy o długości $63\cdot 2 = 126$ (por. tablica 6 na str. 405). Natomiast w przypadku macierzy stowarzyszonej z $(x^6+x^3+1)^2$, tj. z kwadratem wielomianu dzielącego x^9+1, będzie $7\cdot 1 = 7$ cykli o długości $\frac{63}{7} = 9$ i $7\cdot 32 = 224$ cykle o długości $\frac{126}{7} = 18$.

4. Automaty opisywane przez wielomiany typu $f(x) = \varphi_1(x)\cdot\varphi_2(x)\cdot\ldots$

Długości okresów macierzy stowarzyszonych z potęgami wielomianów nierozkładalnych $f(x) = [\varphi(x)]^m$ możemy wyrazić jeszcze inaczej, a mianowicie jeśli $[\varphi(x)]^b$ jest dzielnikiem ciągu $v(x)$, to w wyrażeniu

$$v = v\cdot T^e$$

e jest okresem macierzy stowarzyszonej z wielomianem $\vartheta(x)$

$$\vartheta(x) = \frac{f(x)}{[\varphi(x)]b}.$$

Taki sposób wyrażania długości cyklu jest przydatny w przypadku wielomianów rozkładalnych typu $f(x) = \varphi_1(x)\cdot\varphi_2(x)$. Zilustrujemy to na przykładzie wielomianu $x^5+x^3+x^2+1 = (x^2+x+1)(x+1)^3$. Okres macierzy stowarzyszonej z tym wielomianem jest równy iloczynowi okresów macierzy stowarzyszonych z wielomianami (x^2+x+1) i $(x+1)^3$, tj. równy $3\cdot 4 = 12$. Tak więc każdy ciąg o długości 6 pomnożony przez T^{12} daje ten sam ciąg. Ale istnieją ciągi, które wystarczy pomnożyć przez T^6, T^4, T^3, T^2 lub T, żeby otrzymać taki sam ciąg. Ujęto to w tablicy 8.

TABLICA 8. Długości okresu dla przypadku $f(x) = x^5+x^3+x+1$

Ciąg v jest podzielny przez	Długość okresu	
	równa okresowi macierzy stowarzyszonej z wielomianem	równa
1	$\frac{x^5+x^3+x^2+1}{1} = x^5+x^3+x^2+1$	12
$1+x$	$\frac{x^5+x^3+x^2+1}{x+1} = x^4+x^3+x+1$	6
$1+x+x^2$	$\frac{x^5+x^3+x^2+1}{x^2+x+1} = (x+1)^3$	4
$1+x^2 = (1+x)^2$	$\frac{x^5+x^3+x^2+1}{x^3+1} = x^2+1$	3
$1+x+x^2+x^3 = (1+x)^3$	$\frac{x^5+x^3+x^2+1}{(x+1)^3} = x^2+x+1$	3
$1+x^3 = (1+x+x^2)(1+x)$	$\frac{x^5+x^3+x^2+1}{x^2+1} = x^2+1$	2
$1+x+x^3+x^4 = (1+x+x^2)(1+x^2)$	$\frac{x^5+x^3+x^2+1}{x^4+x^3+x+1} = x+1$	1

Warto wreszcie zauważyć, że macierze quasi-diagonalne

$$\left[\begin{array}{c|cc|c} 1 & 0 & & \\ \hline 0 & 0\,1 & 0 & \\ & 1\,0 & & \\ \hline & 0 & 0\,1 & \\ & & 1\,1 & \end{array}\right], \quad \left[\begin{array}{cc|c|c} 1 & 0 & 0 & \\ 0 & 1 & & 0 \\ \hline & 0 & 1 & \\ \hline & 0 & & 0\,1 \\ & & & 1\,1 \end{array}\right], \quad \left[\begin{array}{ccc|c} 0 & 1 & 0 & \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & \\ \hline & 0 & & 0\,1 \\ & & & 1\,1 \end{array}\right]$$

mają wszystkie te same wielomiany charakterystyczne, równe $x^5+x^3+x^2+1$, ale tylko ostatnia z tych macierzy ma ten sam wielomian minimalny, co omawiana wyżej macierz stowarzyszona z $x^5+x^3+x^2+1$. Tym samym tylko te 2 macierze są podobne, a więc mają te same długości okresów i te same ich liczby.

5. Uwagi o zastosowaniu automatów liniowych.

Automat liniowy opisywany przez macierz stowarzyszoną z wielomianem pierwotnym stopnia m można traktować jako generator niezerowych elementów $GF(2^m)$. Widać to z tablicy związanej z rys. 4, gdzie wyszczególnione są wszystkie (tj. 15) niezerowe elementy $GF(2^4)$. Jeśli dany element oznaczyć przez α^i, to w następnym takcie otrzymamy α^{i+1}; jest to więc układ liczący „w górę". W prosty sposób można zrealizować również układ liczący „w dół". 2 układy: jeden liczący „w górę" a drugi „w dół", pozwalają wykonywać operacje mnożenia i dzielenia elementów $GF(2^m)$ ([9], [11]).

Wyjście dowolnej komórki automatu (p. np. ostatnia kolumna tablicy związanej z rys. 4) możemy traktować jako generator sygnałów pseudoprzypadkowych; w ciągu jednego okresu obserwator nie jest w stanie przewidzieć, czy w następnym takcie pojawi się 0, czy 1.

Bardzo istotne zastosowanie znajdują automaty liniowe w teorii i technice kodów cyklicznych umożliwiających korygowanie błędów w odebranym ciągu ([6], [9], [10]). Lokalizowanie i korygowanie błędnych pozycji związane jest tam z licznymi operacjami algebraicznymi; realizuje się je, praktycznie rzecz biorąc, prawie wyłącznie za pomocą automatów liniowych ([1], [7], [11]).

Prace cytowane

[1] N. M. Abramson, *Error correcting codes from linear sequential circuits*, Fourth London Symposium on Information Theory, Butterworths, London 1961, str. 26-40.

[2] A. A. Albert, *Fundamental concepts of higher algebra*, rozdz. 5, University of Chicago Press, Chicago 1956; tłum. ros. *Конечные поля*, Кибернетический сборник, Новая серия, вып. 3, Мир, Москва 1966, str. 7-49.

[3] G. Birkhoff i S. MacLane, *Przegląd algebry współczesnej*, PWN, Warszawa 1960.

[4] B. Elspas, *The theory of autonomous linear sequential networks*, IRE Trans. Circuit Theory 6 (1959), str. 45-60; tłum. ros. w Кибернетический сборник, вып. 7, Москва 1963, str. 90-128.

[5] B. Gleichgewicht, *Elementy algebry abstrakcyjnej*, PZWS, Warszawa 1966.

[6] D. Gorenstein i N. Zierler, *A class of error correcting codes in p^m symbols*, J. SIAM 9 (1961), str. 207-214.

[7] A. Karczmarewicz, *Zabezpieczenie transmisji przed błędami*, w: *Transmisja danych*, WKŁ, Warszawa 1966, str. 69-102.

[8] A. P. Miszyna i I. W. Proskuriakow, *Algebra wyższa*, PWN, Warszawa 1966.

[9] W. W. Peterson, *Error correcting codes*, MIT Press, Cambridge, Mass., 1961.

[10] J. Seidler, *Teoria kodów*, PWN, Wrocław-Warszawa 1965.

[11] Z. Szwaja, *Dekodowanie binarnych kodów BCH*, Archiwum Automatyki i Telemechaniki 12 (1967), str. 345-369.

Praca wpłynęła 15. 9. 1967

З. ШВАЯ (Познань)

ПРИМЕНЕНИЕ НЕКОТОРЫХ СВОЙСТВ МАТРИЦ НАД $GF(2)$ ДЛЯ ОПИСАНИЯ ЛИНЕЙНЫХ ПЕРЕКЛЮЧАЮЩИХ СХЕМ

РЕЗЮМЕ

В работе исследуются свойства линейных переключающих схем с нулевым входом. Рассматривается следующая проблема: для данного ненулевого состояния схемы определить число тактов, после которых схема возвращается в выходное состояние, если всего 2^m-1 ненулевых состояний (m — число запоминающих ячеек). Схему можно описать уравнением $v_{i+1} = v_i T$, где v_i и v_{i+1} являются последовательностями длины m над $GF(2)$, характеризующими состояния схемы в моментах i и $i+1$, а T квадратной матрицей степени m над $GF(2)$. Проблема сводится к алгебраической задаче определения наименьшего n для которого $v \cdot T^n = v$. Решение этой задачи зависит от полинома, с которым связана матрица T и от соотношения между этим полиномом и последовательностью v. В частом случае, для первообразного полинома над $GF(2)$, соответствующую схему можно рассматривать как образующую ненулевых элементов $GF(2^m)$.

Z. SZWAJA (Poznań)

APPLICATION OF CERTAIN PROPERTIES OF MATRICES OVER $GF(2)$ TO THE DESCRIPTION OF LINEAR SWITCHING NETWORKS

SUMMARY

This paper deals with the autonomous behaviour of linear switching networks. The problem of interest is as follows: given a nonzero state of the network, after how many clock periods does it return to the same state? The circuit can be described by the equation: $v_{i+1} = v_i T$, where v_i and v_{i+1} are states of the network, i. e. sequences of length m over $GF(2)$, at times i and $i+1$, respectively, and T is an $m \times m$ matrix over $GF(2)$. In view of this equation the problem can be stated as follows: what is the smallest integer n such that $v \cdot T^n = v$? The solution depends in general on the polynomial for which T is a companion matrix and on the relation of the sequence v to this polynomial. If in particular this polynomial is primitive over $GF(2)$ then the appropriate network can be treated as a generator of all nonzero elements of $GF(2^m)$.