KYBERNETIKA ČÍSLO 2, ROČNÍK 3/1967

Syntéza a minimalizace regulárních lineárních generátorů*

JOSEF PUŽMAN

V práci se studují vlastnosti jistých matic nad polem dvou prvků definujících regulární lineární autonomní automat a strukturu jeho obvodu (zejména systém zpětných vazeb). Popisuje se algoritmus sestrojení těchto matic k zadanému charakteristickému mnohočlenu tak, aby počet zpětných vazeb byl co nejmenší.

1. ÚVOD

V teorii konečných automatů, která vznikla z potřeb analýzy a syntézy diskrétních soustav a která je již samostatným odvětvím kybernetiky, byl sice udělán značný kus práce, ale stále existuje celá řada nevyřešených otázek a to i v tak úzkém oboru jako je teorie lineárních konečných automatů nebo jen lineárních autonomních automatů. Článek chce proto tuto mezeru částečně zaplnit popsáním jedné metody syntézy a zjednodušení jisté třídy těchto automatů.

Aby se čtenář nemusel seznamovat se základy algebry logiky a obecnou teorií konečných automatů, nebude poukazováno na žádné souvislosti s nimi. Pro naše účely můžeme od podrobného výkladu z hlediska abstraktní teorie automatů zcela upustit. Připomeneme jen, že logická funkce $f(x_1, x_2, \ldots, x_n)$ je lineární, lze-li ji zapsat ve tvaru $a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$, kde sčítání $\oplus$ je mod 2 definované tab. 1 a konstanty $a_1, a_2, \ldots, a_n$ nabývají hodnot 0 nebo 1. *Lineární automat* je pak takový, který lze popsat jen lineárními logickými funkcemi.

Pro praxi má řadu výhod: jednak jej lze snadno realizovat zpožďovacími obvody (posuvným registrem), sčítačkami mod 2 (obvody „nebo exklusive", „nerovnoznačnosti") a konstantami a_i, což znamená trvalé propojení ($a_i = 1$) nebo přerušení ($a_i = 0$) příslušné větve obvodu, a jednak jeho syntéza a analýza se zjednoduší použitím lineární algebry a algebry mnohočlenů.

* Předneseno na semináři *Teorie automatů* pořádaném v Liberci ve dnech 24. — 26. března 1966.

V dalším se budeme výhradně zabývat *lineárními autonomními automaty* čili *lineárními generátory* (autonomními lineárními sekvenčními obvody, ALSC), což jsou automaty bez vstupu, samočinně generující nějakou výstupní posloupnost v závislosti jen na vnitřních stavech. Ty se obecně definují polem $\mathscr{P}$ h prvků, kde h je prvočíslo (v našem případě $\mathscr{P}$ je pole dvou prvků 0 a 1, neboť 0 vzhledem ke sčítání mod 2 a 1 vzhledem k obyčejnému násobení tvoří pole), n-rozměrným vektorovým prostorem $\mathscr{S}$ s prvky $[S_i]$, $i = 1, 2, \ldots, 2^n$, nad polem $\mathscr{P}$ (prostor vnitřních stavů)

Tabulka 1.

Pravidla sčítání mod 2

x_2	x_1	$x_1 \oplus x_2$
0	0	0
0	1	1
1	0	1
1	1	0

a maticí $[T]$ n-tého řádu nad polem $\mathscr{P}$ určující závislost stavu v každém okamžiku na stavu v předchozím okamžiku [2]. Existuje-li mimoto ke každému stavu jediný stav předchozí, probíhají vnitřní stavy lineárního generátoru cykly obsahující všechny stavy; takový lineární generátor se nazývá *regulárním* na rozdíl od singulárního lineárního generátoru, který může přejít do některého stavu z více stavů předchozích. Protože v dalším nebudeme singulární lineární generátory uvažovat, výraz regulární často vynecháme.

Nezáleží-li na struktuře (sledu) vnitřních stavů v cyklech, lze všechny lineární generátory rozdělit do tříd podle délek jednotlivých cyklů. Označíme-li délky cyklů přirozenými čísly $k_1, k_2, \ldots, k_r$, přičemž $\sum_{i=1}^{r} k_i = 2^n$, pak třídu lineárních generátorů lze definovat množinou cyklů $\{k_1, k_2, \ldots, k_r\}$ [1]. V rámci jedné třídy se lineární generátory liší jen posloupností stavů v cyklech, tj. kódováním vnitřních stavů.

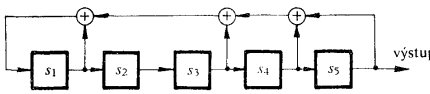
Zvláštní třídu tvoří tzv. *lineární generátory maximálních posloupností* (m-posloupností [1], posloupností maximální délky [5]) definovanou dvojicí $\{1, 2^n - 1\}$, jejichž množina stavů se rozpadá na nulový cyklus délky 1 (obvod je trvale v nulovém stavu) a maximální cyklus délky $2^n - 1$ (obvod probíhá všechny stavy kromě nulového). Na vlastnosti maximálních posloupností bylo poukázáno již dříve (v r. 1955 upozornil S. W. Golomb na jejich statistickou strukturu a na možnosti jejich využití jako pseudonáhodných posloupností), ale teprve v poslední době se tyto posloupnosti a jejich generátory studují soustavněji zejména v souvislosti s generováním cyklických kódů [3, 4, 7, 9].

Protože tento stručný úvod není dostačující pro toho, kdo se lineárními generátory podrobněji nezabýval, probereme v dalších dvou částech některé výsledky podrobněji (pro lepší názornost na příkladě). Vlastní syntéze a minimalizaci je pak věnována část 4 a části následující.

2. STRUKTURNÍ MATICE LINEÁRNÍHO GENERÁTORU

Jak je obvyklé [1, 5], budeme realizovat lineární generátor n-členným posuvným registrem (n zpožďovacími obvody v kaskádě) s určitým systémem vazeb.

Na obr. 1 je znázorněn pětičlenný posuvný registr se 4 zpětnými vazbami a 3 sčítačkami mod 2. Protože každý zpožďovací obvod může být jen ve stavu 0 nebo 1,



Obr. 1. Schéma lineárního generátoru se sčítačkami mod 2 vně posuvného registru.

jsou jednotlivé stavy celého posuvného registru dány pětirozměrným vektorem (v pořadí zpožďovacích obvodů) $[s_1, s_2, s_3, s_4, s_5]$, kde $s_i = 0$ nebo 1, přičemž celkový počet stavů je $2^5 = 32$.

Analyzujme podrobněji chování obvodu. Z obr. 1 je ihned vidět, že při počátečním stavu $[0, 0, 0, 0, 0]$ zůstane obvod trvale v tomto nulovém stavu, tj. realizuje cyklus 00000 ... Zkusme jiný počáteční stav, např. $[0, 0, 0, 0, 1]$ odpovídající desítkové jedničce. V následujícím taktu se stav 1 změní ve stavu 16 $[1, 0, 0, 0, 0]$, ten přejde ve stav 24 $[1, 1, 0, 0, 0]$, atd., až posledním 31-ním stavem 3 $[0, 0, 0, 1, 1]$ je cyklus ukončen, neboť obvod se opět dostává do stavu 1 (tab. 2). Protože obvod na obr. 1 realizuje dva cykly (nulový a maximální), představuje lineární generátor maximální posloupnosti, který patří do třídy $\{1, 31\}$.

Na obr. 1 jsou jednotlivé zpožďovací obvody označeny jako dvojkové proměnné s_1 až s_5. Označíme-li čárkou stav v následujícím okamžiku (taktu), platí pro náš příklad tato soustava lineárních logických rovnic:

$$
\begin{aligned}
s_1' &= s_1 \oplus \quad s_3 \oplus s_4 \oplus s_5 \,, \\
s_2' &= s_1 \,, \\
s_3' &= \quad s_2 \,, \\
s_4' &= \quad\quad s_3 \,, \\
s_5' &= \quad\quad\quad s_4 \,,
\end{aligned}
$$

Tabulka 2.

Struktura cyklu maximální délky

stav s_1	s_2	s_3	s_4	s_5	číslo stavu
0	0	0	0	1	1
1	0	0	0	0	16
1	1	0	0	0	24
0	1	1	0	0	12
1	0	1	1	0	22
0	1	0	1	1	11
1	0	1	0	1	21
0	1	0	1	0	10
0	0	1	0	1	5
1	0	0	1	0	18
0	1	0	0	1	9
0	0	1	0	0	4
0	0	0	1	0	2
1	0	0	0	1	17
0	1	0	0	0	8
1	0	1	0	0	20
1	1	0	1	0	26
1	1	1	0	1	29
1	1	1	1	0	30
1	1	1	1	1	31
0	1	1	1	1	15
1	0	1	1	1	23
1	1	0	1	1	27
0	1	1	0	1	13
0	0	1	1	0	6
1	0	0	1	1	19
1	1	0	0	1	25
1	1	1	0	0	28
0	1	1	1	0	14
0	0	1	1	1	7
0	0	0	1	1	3
0	0	0	0	1	1

kterou lze zapsat v maticovém tvaru jako

$$\begin{bmatrix} s'_1 \\ s'_2 \\ s'_3 \\ s'_4 \\ s'_5 \end{bmatrix} = \begin{bmatrix} 10111 \\ 10000 \\ 01000 \\ 00100 \\ 00010 \end{bmatrix} . \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \end{bmatrix}$$

$$[S'] = [T] \cdot [S],$$

kde $[T]$ je matice n-tého (v našem případě pátého) řádu nad polem dvou prvků 0 a 1. Ze stavu $[s'_1, s'_2, s'_3, s'_4, s'_5]$ lze stejným způsobem přejít k dalšímu stavu $[s''_1, s''_2, s''_3, s''_4, s''_5] : [S''] = [T][S'] = [T][T][S] = [T]^2[S]$ atd., takže obecně $[S^k] = [T]^k[S]$. Za předpokladu existence inverzní matice $[T]^{-1}$ lze z rovnice $[S'] = [T][S]$ jednoznačně určit k danému stavu $[S']$ stav předchozí $[S]$. Proto nutnou a postačující podmínkou pro regularitu lineárního generátoru daného maticí $[T]$ je rovnost $|T| = 1$ (obecně $|T| \neq 0$, ale pro determinant nad polem dvou prvků platí $|T| = 0$ nebo 1). Kritérium však vyžaduje vyčíslení determinantu, což pro velká n není snadné a proto zformulujeme jednodušší prověrku regulárnosti.

Lemma 1. *Lineární generátor je regulární tehdy a jen tehdy, obsahuje-li jeho matice* $[T]$ *jen vzájemně lineárně nezávislé sloupce a řádky, jinými slovy, žádný řádek nesmí být nulový a v matici se nesmí vyskytovat* 2 *stejné řádky či sloupce.*

Důkaz plyne z definice regularity lineárního generátoru a z vlastností determinantu [6] nad polem dvou prvků.

Všimněme si podrobněji matice $[T]$. Je charakterizována zejména nenulovou úhlopříčkou pod hlavní úhlopříčkou (s prvky $t_{ij} = 1$ pro $i = j + 1, j = 1, 2, \ldots, n - 1$) odpovídající vlastnímu posuvnému registru a systémem prvků v prvním řádku ($t_{ij} = c_{n-j} = 0$ nebo 1, $j = 1, 2, \ldots, n$) odpovídajícím zpětným vazbám obvodu (ostatní prvky jsou nulové). Obecně má tedy matice $[T]$ tvar (pro typ obvodu na obr. 1)

(C)
$$[T] = \begin{bmatrix} c_{n-1} & c_{n-2} & \ldots & c_1 & c_0 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & 0 \end{bmatrix},$$

kde $c_i = 1$ znamená zpětnou vazbu z $(n - i)$-tého zpožďovacího obvodu do prvního. Je ihned vidět, že pro libovolné prvky c_i jsou všechny řádky i sloupce vzájemně lineárně nezávislé s výjimkou, je-li $c_0 = 0$, posledního sloupce (v některých případech i prvního řádku). Budeme-li požadovat $c_0 = 1$ (což ve schématu představuje zavedení „nejlepší" zpětné vazby z n-tého zpožďovacího obvodu do prvního), bude podle lemmatu 1 lineární generátor daný maticí $[T]$ typu (C) vždy regulární.

Aby nebylo třeba sestrojovat celý stavový diagram a hledat délky k_i jednotlivých stavových cyklů, stačí řešit vztahy $[S^j] = [T]^{k_i}[S^j]$ pro určité $[S^j]$ a nejmenší k_i. Zejména v triviálním případě, je-li $[S^j] = [0]$ (nulový stav), je podmínka splněna pro $k_i = 1$ a pro každé $[T]$, takže každý lineární regulární generátor probíhá nulový cyklus délky 1. Pro maximální cyklus (existuje-li pro dané $[T]$) musí platit $[T]^{2^n-1} = [I]$, kde $[I]$ je jednotková matice. Obecně však závisí nejen na matici $[T]$, ale i na volbě počátečního stavu.

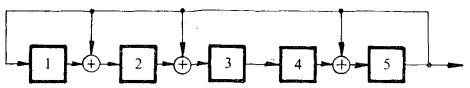
Kromě schématu na obr. 1 se běžně užívá ještě další typ obvodu realizující lineární generátor: obvod se sčítačkami mod 2 rozmístěnými uvnitř posuvného registru. Pro náš příklad je znázorněn na obr. 2. Není obtížné analýzou obvodu si ověřit jeho chování. Přestože se schémata na obr. 1 a 2 od sebe zásadně liší, představují lineární generátor se shodnými délkami cyklů, takže oba lineární generátory patří do téže třídy $\{1, 31\}$.

Změnou schématu se však mění i matice $[T]$. Její tvar je obecně

$$(B) \qquad [T] = \begin{bmatrix} 0 & 0 & \dots & 0 & b_0 \\ 1 & 0 & \dots & 0 & b_1 \\ 0 & 1 & \dots & 0 & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & b_{n-1} \end{bmatrix},$$

kde $b_i = 1$ označuje zpětnou vazbu z n-tého zpožďovacího obvodu do i-tého. Všimněme si, že matice typu (B) vznikla z matice typu (C) překlopením podle vedlejší

Obr. 2. Schéma lineárního generátoru se sčítačkami mod 2 uvnitř posuvného registru.



úhlopříčky, takže stačí mluvit o jediné matici $[T]$ (typu (C) resp. (B)) a o matici k ní duální (typu (B) resp. (C)).

Z analýzy schématu a jeho příslušné matice vyplyne jejich souvislost. Prvky t_{ij} matice $[T]$ jsou rovny 0 nebo 1 podle toho, není-li nebo je-li i-tý zpožďovací obvod napájen j-tým zpožďovacím obvodem, což platí i pro obecný lineární obvod, jak se lze snadno přesvědčit soustavou lineárních logických rovnic. Protože matice $[T]$ jednoznačně definuje strukturu příslušného obvodu, nazveme ji *strukturní*. Dále, protože ze strukturní matice $[T]$ lze určit délky stavových cyklů, tj. množinu $\{k_1, k_2, \dots, k_r\}$, charakterizuje matice $[T]$ příslušnost lineárního generátoru ke třídě $\{k_1, k_2, \dots, k_r\}$.

3. CHARAKTERISTICKÝ MNOHOČLEN LINEÁRNÍHO GENERÁTORU

Zjistit délky cyklů ze strukturní matice $[T]$ není příliš snadné. Zkoumání matice $[T]$ lze však převést na zkoumání jejího charakteristického mnohočlenu $f(X)$ [1]. Ke každé čtvercové matici $[T]$ existuje jediný charakteristický mnohočlen, daný determinantem charakteristické matice $X[I] - [T]$, takže pro matici nad polem dvou prvků je $f(X) = |X[I] \oplus [T]| = X^n \oplus a_{n-1}X^{n-1} \oplus \dots \oplus a_1X \oplus a_0$, kde $a_i = 0$ nebo 1. Koeficienty a_i jsou dány [6] součtem všech hlavních minorů i-tého řádu, tj. součtem všech minorů i-tého řádu souměrně rozložených podél hlavní úhlopříčky; zejména $a_{n-1} = q_T$ (q_T je součet prvků na hlavní úhlopříčce) a $a_0 = |T|$

(regulárnost matice $[T]$ je tedy ekvivalentní vztahu $a_0 = 1$). Nás však bude zajímat výpočet charakteristického mnohočlenu matice typu (C) a (B):

$$f(X) = X^n \oplus c_{n-1}X_n^{-1} \oplus \ldots \oplus c_1 X \oplus 1 \quad \text{pro typ } (C) \text{ a}$$
$$f(X) = X^n \oplus b_{n-1}X^{n-1} \oplus \ldots \oplus b_1 X \oplus 1 \quad \text{pro typ } (B),$$

tj. prvky c_i resp. b_j v prvním řádku resp. v n-tém sloupci jsou přímo koeficienty charakteristického mnohočlenu. Pro předchozí příklad je $f(X) = X^5 \oplus X^4 \oplus X^2 \oplus X \oplus 1$.

Význam charakteristického mnohočlenu je dán větou Hamiltonovou-Cayleyovou [6] dokazující, že každá matice $[T]$ je kořenem svého charakteristického mnohočlenu $f(X)$ čili $f([T]) = [0]$. Pomocí této věty lze algebraicky studovat chování lineárního generátoru, zejména délky cyklů k_i (podrobněji o tom viz [1]; my se zde omezíme jen na několik nejdůležitějších výsledků).

Nazveme mnohočlen $f(X)$ nad polem libovolných prvků *rozložitelným*, existují-li mnohočleny $f_1(X)$ a $f_2(X)$ nad týmž polem takové, že $f(X) = f_1(X) f_2(X)$, v opačném případě je $f(X)$ nerozložitelný. Dále nazveme nerozložitelný mnohočlen $f(X)$ *primitivním*, není-li dělitelem mnohočlenu $X^k - 1$ pro všechna $k < 2^n - 1$. Platí [1, 7]: *Lineární generátor daný maticí* $[T]$ *generuje posloupnost maximální délky tehdy a jen tehdy, je-li charakteristický mnohočlen matice* $[T]$ *nerozložitelný a primitivní.* Podrobněji o počtu nerozložitelných a primitivních mnohočlenů pro dané n a o jejich nalezení viz v [1]; v [7] je uveden přehled všech nerozložitelných mnohočlenů s označením mnohočlenů primitivních pro $n \leqq 16$. (Mnohočlen $X^5 \oplus X^4 \oplus X^2 \oplus X \oplus 1$ z našeho příkladu je nerozložitelný a primitivní a skutečně představuje lineární generátor maximální posloupnosti.)

Jaká je souvislost mezi charakteristickým mnohočlenem a strukturní maticí $[T]$? V algebře se nazývá matice typu (C) nebo (B) nad polem libovolných prvků konjugovanou maticí k mnohočlenu $f(X)$ nad týmž polem, přičemž charakteristický mnohočlen konjugované matice je totožný s jejím minimálním mnohočlenem* a je roven $f(X)$. A dále platí [1]: *Je-li charakteristický mnohočlen* $f(X)$ *strukturní matice* $[T]$ *roven minimálnímu mnohočlenu téže matice, určuje jednoznačně příslušnost lineárního generátoru daného maticí* $[T]$ *ke třídě* $\{k_1, k_2, \ldots, k_r\}$.

Různé způsoby vyjádření lineárního generátoru jsou velmi výhodné. Mnohočleny $f(X)$ se snadno studují algebraickými metodami, zatímco strukturní matice $[T]$ je vhodná pro syntézu skutečných obvodů. Charakteristický mnohočlen má také význam pro analýzu vnějšího chování lineárního generátoru.

Zatím jsme studovali lineární generátory jen z hlediska vnitřní struktury bez ohledu na výstup. Můžeme se však na ně dívat jako na „černou schránku", tj. sledovat jen výstup. Je zřejmé, že výstupní posloupnost regulárního lineárního generátoru bude též tvořit cykly o délkách shodných se stavovými cykly. K určení struktury

* Minimální mnohočlen matice $[T]$ je nulový mnohočlen $\varphi(X)$ (tj. pro nějž $\varphi([T]) = [0]$) nejnižšího stupně.

cyklů se zavádí D-operátory a zpožďovací mnohočlen $F(D)$ [5]. Je-li n počet zpožďovacích obvodů (2^n – počet vnitřních stavů) lineárního generátoru, je $F(D)$ n-tého stupně a $(n + 1)$-ní symbol výstupní posloupnosti je jednoznačně dán aplikací zpožďovacího mnohočlenu $F(D)$ na n předchozích symbolů. Vztah mezi $f(X)$ a $F(D)$ je následující: $F(D) = D^n f(1/D)$ resp. $f(X) = X^n F(1/X)$. Pro náš příklad ($f(X) = X^5 \oplus X^4 \oplus X^2 \oplus X \oplus 1$) má zpožďovací mnohočlen tvar $F(D) = 1 \oplus D \oplus D^3 \oplus D^4 \oplus D^5$, takže maximální výstupní posloupnost je 0000111001101111101 0001001010110000 1 ...

4. SMÍŠENÁ STRUKTURNÍ MATICE

Z předchozího již můžeme formulovat úlohu syntézy lineárních generátorů. Prakticky se může jednat o řešení dvou problémů: nalézt lineární generátor patřící do dané třídy $\{k_1, k_2, \ldots, k_r\}$ nebo nalézt lineární generátor s daným výstupem. K řešení prvního problému se ihned nabízí algebraické metody pomocí charakteristického mnohočlenu $f(X)$; dalším krokem je konstrukce strukturní matice $[T]$, k níž by byl $f(X)$ minimální. Druhý problém vyžaduje buď zadání všech cyklů výstupní posloupnosti nebo zpožďovacího mnohočlenu $F(D)$ (způsob určení $F(D)$ z výstupní posloupnosti je v [5]), a protože k $F(D)$ jednoznačně existuje $f(X)$, zbývá opět zkonstruovat strukturní matici $[T]$. Konstrukce strukturní matice nečiní potíže v případě matic typu (B) nebo (C), které však nedávají možnost nalezení prakticky „jednoduchého" schématu. Abychom zpřesnili poslední termín, zaveďme pojem *složitosti* lineárního generátoru.

Počet vnitřních stavů a tedy i počet zpožďovacích obvodů je pevně dán příslušností lineárního generátoru k určité třídě příp. mnohočlenem $F(D)$. Z obr. 1 a 2 a z matice typu (B) a (C) je zřejmá úloha sčítaček mod 2: sčítačky je potřeba ke sloučení dvou vazeb směřujících do téhož zpožďovacího obvodu, což v termínech strukturní matice znamená, že počet sčítaček mod 2 např. i-tého zpožďovacího obvodu je dán počtem nenulových prvků v i-tém řádku matice $[T]$ zmenšený o jedničku. Je-li lineární generátor realizován posuvným registrem, je zcela přirozené volit za míru složitosti počet p všech vazeb (obecně dopředných a zpětných) nebo počet sčítaček mod 2 (těch je nejvýše $p - 1$). Přítomnost posuvného registru se ve strukturní matici projeví jedničkovou úhlopříčkou pod hlavní úhlopříčkou, takže počet zpětných vazeb je dán počtem všech nenulových prvků matice $[T]$ zmenšeným o $n - 1$.

Protože strukturní matice úzce souvisí s charakteristickým mnohočlenem $f(X)$, je výhodné zavést i složitost (délku) p' mnohočlenu jako počet nenulových koeficientů a_i. V případě strukturní matice typu (B) resp. (C) je $p = p'$; jak však uvidíme dále, existují matice $[T]$ k $f(X)$ takové, že $p \leqq p'$.

Úloha společná oběma problémům syntézy je tedy následující: naléz k danému $f(X)$ n-tého stupně nad polem 2 prvků matici n-tého řádu nad týmž polem takovou, aby její charakteristický mnohočlen byl identický s minimálním a byl roven $f(X)$ a aby její složitost p byla co nejmenší (nebo alespoň, aby $p \leqq p'$).

Zde se nebudeme zabývat řešením této obecné úlohy, ale zredukujeme ji na následující: nalézt regulární matici $[T]$ nad polem dvou prvků takovou, aby její charakteristický mnohočlen byl identický s minimálním a byl snadno vyčíslitelný, aby bylo možno dosáhnout $p \leqq p'$, a případně aby matice typu (B) a (C) byly jejím zvláštním případem. Chceme-li dodržet podmínku realizace lineárního generátoru posuvným registrem se systémem vazeb, požadujeme nakonec, aby úhlopříčkové prvky hledané matice pod hlavní úhlopříčkou byly jedničkové.

Jako jedno z řešení se zcela přirozeně nabízí zavést následující matici, kterou nazveme *smíšenou* typu (BC).

Definice 1. Smíšená matice $[T]$ typu (BC) n-tého řádu nad polem 2 prvků je definována prvky: $t_{ij} = 1$ pro $i = j + 1, j = 1, 2, \ldots, n - 1$; $t_{ij} = c_{n-j}$, $t_{in} = b_{i-1}$, $i, j = 1, 2, \ldots, n$, $b_i, c_j = 0$ nebo 1; $t_{ij} = 0$ v ostatních případech, tj. má tvar

$$(BC) \qquad [T] = \begin{bmatrix} c_{n-1} & c_{n-2} & \ldots & c_1 & b_0 \\ 1 & 0 & \ldots & 0 & b_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \ldots & 1 & b_{n-1} \end{bmatrix}.$$

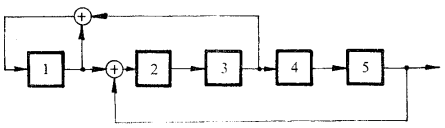
Určíme její charakteristický mnohočlen $f(X)$: $f(X) = \left|[T] \oplus X[I]\right| = X^n \oplus$ $\oplus X^{n-1}(c_{n-1} \oplus b_{n-1}) \oplus \ldots \oplus X(c_1 \oplus b_1) \oplus b_0 \oplus X^{n-2}c_{n-1}b_{n-1} \oplus X^{n-3}(c_{n-1}b_{n-2} \oplus$ $\oplus c_{n-2}b_{n-1}) \oplus \ldots \oplus X(c_{n-1}b_2 \oplus c_{n-2}b_3 \oplus \ldots \oplus c_1 b_{n-2}) \oplus c_{n-1}b_1 \oplus c_{n-2}\ b_2 \oplus$ $\oplus \ldots \oplus c_1 b_{n-1} = X^n \oplus a_{n-1}X^{n-1} \oplus \ldots \oplus a_1 X \oplus a_0$, kde $a_{n-i} = \sum_{j=0}^{i} c_{n-j}b_{n-i+j} \bmod 2$, $c_n = b_n = 1$ a $c_0 = 0$. Nutná a postačující podmínka pro regularitu matice $[T]$ typu (BC) je tedy rovnost $\sum_{j=0}^{n-1} c_{n-j}b_j = 1 \bmod 2$.

Ukažme, že matice typu (BC) splňuje podmínku $p \leqq p'$ (zatím na příkladě). Opět použijeme lineárního generátoru daného charakteristickým mnohočlenem $f(X) = X^5 \oplus X^4 \oplus X^2 \oplus X \oplus 1$ a budeme hledat smíšenou strukturní matici $[T]$, která by splňovala definici 1 a jejíž charakteristický mnohočlen by byl roven $f(X)$. Tomu vyhovuje např. matice

$$\begin{bmatrix} 10100 \\ 10001 \\ 01000 \\ 00100 \\ 00010 \end{bmatrix},$$

jejíž složitost $p = 3 < p' = 4$. Příslušné schéma lineárního generátoru je na obr. 3 a od obr. 1 a 2 se liší menším počtem sčítaček mod 2. Je samozřejmé, že i tento generátor patří do třídy $\{1, 31\}$, neboť má shodný charakteristický mnohočlen s oběma předchozími a ze stejného důvodu mají všechny tři obvody stejný výstup.

Protože smíšená matice bude výchozí k syntéze a k zjednodušení počtu zpětných vazeb lineárních generátorů, zformulujme podrobněji její vlastnosti.



Obr. 3. Minimální schéma lineárního generátoru maximální posloupnosti ze třídy $\{1,31\}$.

Věta 1. *a) Smíšená matice* $[T]$ *typu* (BC) *nad polem* 2 *prvků n-tého řádu je regulární tehdy a jen tehdy, jestliže*

$$\sum_{j=0}^{n-1} c_{n-j} b_j = 1 \,, \quad \mathrm{mod}\ 2 \quad (c_n = 1) \,.$$

b) Charakteristický mnohočlen smíšené matice $[T]$ *je identický s minimálním mnohočlenem a je roven*

$$f(X) = X^n \oplus a_{n-1} \oplus \ldots \oplus a_1 X \oplus a_0 \,,$$

kde

$$a_{n-i} = \sum_{j=0}^{i} c_{n-j} b_{n-i+j} \ \mathrm{mod}\ 2 \,,$$

přičemž $c_n = b_n = 1$, $c_0 = 0$.

c) Překlopením smíšené matice $[T]$ *podle vedlejší úhlopříčky vznikne duální matice s týmž charakteristickým* (a tedy i minimálním) *mnohočlenem.*

Je třeba dokázat pouze tvrzení b). Aby platila rovnost mezi charakteristickým a minimálním mnohočlenem, je nutné a stačí, aby největší společný dělitel minorů $(n-1)$-ního řádu charakteristické matice $[T] \oplus X[I]$ byl roven 1 [6]. Stačí tedy nalézt alespoň jeden takový minor, jehož charakteristický mnohočlen je roven 1 a tím je minor M_{1n}, který je determinantem trojúhelníkové matice $(n-1)$-ního řádu s jedničkami na hlavní úhlopříčce, takže 1 je největší společný dělitel a oba mnohočleny jsou identické.

5. SYNTÉZA SMÍŠENÉ MATICE

Z vlastností smíšené strukturní matice $[T]$, zejména z tvaru jejího charakteristického mnohočlenu, je již zřejmý způsob redukce zpětných vazeb lineárního generátoru. Je-li např. $c_i = b_j = 1$ pro některé $i \neq j$ a současně $c_k = b_l = 0$ pro všechna $k \neq i$, $l \neq j$, má charakteristický mnohočlen tvar $f(X) = X^n \oplus c_i X^i \oplus b_j X^j \oplus c_i b_j X^{i+j-n}$, kde $c_i b_j = 0$ pro $i + j < n$. Délka charakteristického mnohočlenu $f(X)$ pro $i + j \geqq n$ je $p' = 3$, složitost strukturní matice $[T]$ je $p = 2$. S rostoucím počtem nenulových prvků c a b matice $[T]$ může sice klesat složitost p, ale zá-

roveň stoupá obtížnost rychlého určení charakteristického mnohočlenu. Navíc zjednodušení počtu zpětných vazeb vyžaduje řešení obrácené úlohy: k danému mnohočlenu $f(X)$ n-tého stupně nalézt rozložení nejmenšího počtu prvků c a b smíšené strukturní matice $[T]$ n-tého řádu tak, aby její charakteristický mnohočlen byl totožný s mnohočlenem $f(X)$, jinými slovy, aby pro koeficienty a mnohočlenu $f(X)$ byla splněna soustava n rovnic (nad polem dvou prvků):

$$(1) \qquad \sum_{j=0}^{i} c_{n-j} b_{n-i+j} = a_{n-i} \bmod 2\,, \quad i = 1, 2, \ldots, n\,,$$

kde $c_n = b_n = 1$, $c_0 = 0$, za předpokladu, že počet nenulových prvků c a b je minimální.

Není obtížné nalézt pro danou délku p' mnohočlenu $f(X)$ nejmenší možnou hodnotu p strukturní matice, jestliže si uvědomíme, že p_1 nenulových prvků c a p_2 nenulových prvků b může realizovat až $p_1 + p_2 + p_1 p_2$ koeficientů a mnohočlenu $f(X)$. Není však známa rychlá metoda určení nejmenší složitosti p k libovolnému mnohočlenu a ani obecné kritérium, zda lze sestrojit matici $[T]$ k $f(X)$ tak, aby $p < p'$. Přesto se pokusíme zformulovat několik pravidel, která zaručí zmenšení nebo alespoň nezvětšení složitosti, i když obecně nemusí vést k minimálnímu tvaru.

Vychází se přímo ze soustavy n rovnic. Jestliže řešení probíhá jednotlivé rovnice pro $i = 1, 2, \ldots, n$, pak i-tá rovnice (za předpokladu určení prvků b_{n-l}, c_{n-l} pro všechna $l < i$) má tvar $b_{n-i} \oplus c_{n-i} = a'_{n-i}$, kde $a'_{n-i} = a_{n-i}$ nebo $a_{n-i} \oplus 1$. Podle hodnoty koeficientu a_{n-i} mohou tedy nastat dva případy: $b_{n-i} = c_{n-i}$ nebo $b_{n-i} \neq c_{n-i}$. Je-li p' malé, pak je zcela přirozené v prvním případě volit $b_{n-i} = c_{n-i} = 0$ (je-li $a_{n-i} = 1$, došlo k realizaci koeficientu a_{n-i} některými prvky b_{n-j}, c_{n-j}, $j, k < i$; v opačném případě se složitost nemění), pro $p' \geqq 6$ však i volba $b_{n-i} = c_{n-i} = 1$ může vést ke zjednodušení, zejména, jestliže b_{n-i} a c_{n-i} spolu s některými prvky b_{n-j}, c_{n-k}, $j, k > i$, realizují více než dva koeficienty a. V druhém případě (pro $b_{n-i} \neq c_{n-i}$) je dvojice prvků neurčitá (dočasně se volí např. $c_{n-i} = 1 \neq b_{n-i} = 0$) a teprve řešení dalších rovnic ji může definitivně určit. Nazveme tuto dvojici *volnou*. Jsou-li výsledkem řešení první až $(i-1)$-ní rovnice některé volné dvojice, pak i-tá rovnice může nebo nemusí záviset na některé z nich. Závisí-li alespoň na jedné volné dvojici, pak vhodným určením lze docílit $b_{n-i} = c_{n-i}$; i tento případ vede pro $a_{n-i} = 1$ ke zjednodušení. Je-li nakonec i-tá rovnice tvaru $c_{n-i} \neq b_{n-i}$ a nezávislá na žádné volné dvojici a současně $a_{n-i} = 0$, pak došlo v i-tém kroku k relativnímu zvětšení složitosti a závisí tedy na konečné hodnotě p, zda je menší nebo větší než p'. Je-li $p > p'$ a protože volbou např. všech $c_{n-i} = 1$ pro $a_{n-i} = 1$ dojdeme k rovnici typu (C), přičemž $p = p'$, pak v celé soustavě rovnic musí existovat alespoň jediná (např. j-tá) tvaru $c_{n-j} \oplus b_{n-j} = 1$ závislá na některé volné dvojici, která byla určena tak, aby $c_{n-j} = b_{n-j}$. Jestliže nyní postupným opakováním řešení soustavy rovnic s tím, že v posledních případech určíme volné dvojice, aby $c_{n-j} \neq b_{n-j}$, musí mezi všemi řešeními existovat alespoň jediné, pro které $p \leqq p'$.

Tím jsme dokázali

Větu 2. *Použitím následujících pravidel k soustavě n rovnic* (1) *nad polem dvou prvků docílíme* $p \leqq p'$:

a) Jestliže při řešení i-té rovnice vyjde $c_{n-i} = b_{n-i}$, *položí se* $c_{n-i} = b_{n-i} = 0$.

b) Jestliže při řešení i-té rovnice vyjde $c_{n-i} \neq b_{n-i}$ *a současně i-tá rovnice je závislá alespoň na jedné volné dvojici* $b_{n-j}, c_{n-j}, j < i$, *provede se její konečné určení tak, aby bylo možno použít pravidla a). Je-li současně* $a_{n-i} = 1$, *rovnice se označí* (*např.* *).

c) Není-li použitelné pravidlo a) nebo b), jsou $c_{n-i} \neq b_{n-i}$ *volnou dvojicí.*

d) Po vyřešení celé soustavy n rovnic s použitím pravidel a) až c) (zejména je-li $p > p'$), *zkoumají se postupně další varianty řešení, počínaje označenými rovnicemi, volbou volných dvojic tak, aby k označeným rovnicím bylo použitelné pravidlo c).*

Protože pravidla nezaručují všechny možné varianty rozložení prvků b_{n-i}, c_{n-i} pro daný charakteristický mnohočlen, nemohou zaručit nalezení všech minimálních tvarů nebo vůbec nalezení minimálního tvaru (vylučují $c_{n-i} = b_{n-i} = 1$). V praktických případech jsou však použitelná a dosažené výsledky obvykle vyhovují. Probrání všech variant by totiž neúměrně prodloužilo řešení pro všechny minimální tvary, které prakticky není třeba ani znát a rychlejší algoritmus se nepodařilo nalézt.

Použijme pravidel ke zjednodušení pro náš příklad $f(X) = X^5 \oplus X^4 \oplus X^2 \oplus \oplus X \oplus 1$. Soustava rovnic má tvar:

$$
\begin{aligned}
b_4 \oplus c_4 &= 1\,, \\
b_3 \oplus b_4 c_4 \oplus c_3 &= 0\,, \\
(*) \qquad b_2 \oplus b_3 c_4 \oplus b_4 c_3 \oplus c_2 &= 1\,, \\
b_1 \oplus b_2 c_4 \oplus b_3 c_3 \oplus b_4 c_2 \oplus c_1 &= 1\,, \\
b_0 \oplus b_1 c_4 \oplus b_2 c_3 \oplus b_3 c_2 \oplus b_4 c_1 &= 1\,.
\end{aligned}
$$

Jestliže v označené rovnici, závisející na volné dvojici b_2, c_2 a b_4, c_4, položíme $b_2 = = c_4 = 1$ resp. $b_4 = c_2 = 1$, lze k ní použít pravidla a) a v obou případech vyjde $b_0 = 1$. Další varianta vznikne volbou $b_2 = b_4 = 1$ resp. $c_2 = c_4 = 1$, kdy $b_1 \neq c_1$ a z poslední rovnice pro $b_0 = 0$ dostaneme $c_1 = 1$ resp. $b_1 = 1$. Ve všech čtyřech případech je výsledný tvar stejně složitý a je skutečně minimální (neboť $p' = 4 < 6$, takže řešení $b_i = c_i = 1$ nemůže vést k jednodušššímu tvaru).

Ruční výpočet soustavy n rovnic pro velká n je nemožný a pro malá n značně zdlouhavý. Je-li p' malé (např. $p' < 6$), je rychlejší sestrojit matici $[T]$ přímo podle metody realizace koeficientů a_i, a_j a a_{i+j-n} uvedené výše. Protože je zbytečné zapisovat celou matici $[T]$, stačí vypsat jen první řádek a n-tý sloupec (tab. 3) se společným okénkem pro $b_0 = c_0$ a okénka označit pro rychlejší orientaci mocninami X. Do jednotlivých okének řádku b resp. c se pak zapisují jedničky označující nenulové prvky b_i resp. c_j. Je-li např. zapsán prvek b pro X^i a c_j pro X^j, pak tato dvojice

realizuje v mnohočlenu $f(X)$ koeficienty a_i při X^i, a_j při X^j a a_{i+j-n} při X^{i+j-n} v případě, že $i + j \geqq n$; v opačném případě, tj. pro $i + j < n$ realizace nenastává.

Protože tímto způsobem využíváme jen pravidla a), c) a částečně b), nedojdeme obecně k minimálnímu tvaru. Avšak pro malé p' lze vždy probrat všechny varianty a pro velká p' stačí obvykle alespoň zjednodušení.

Tabulka 3.

Tabulka pro minimalizaci

	X^{n-1}	X^{n-2}	X^{n-3}	...	X^3	X^2	X	1
c								
b								

Sestrojíme tabulku opět pro náš příklad. V tab. 4 je jeden minimální tvaru znázorněn. Nenulové prvky odpovídají koeficientům při X^4, X^2, X a $X^0 = 1$ (neboť $X^{4+1-5} = X^0$). Nelze však zaměnit v tab. 4 prvek c_2 prvkem b_2, neboť výsledkem

Tabulka 4.

Minimalizace $f(X) = X^5 \oplus X^4 \oplus X^2 \oplus X \oplus 1$

	X^4	X^3	X^2	X	1
c	1		1		
b				1	

by byly nenulové koeficienty při X^4, X^2, $X^{4+1-5} = 1$ a $X^{4+2-5} = X$ a charakteristický mnohočlen by měl tvar $X^5 \oplus X^4 \oplus X^2 \oplus 1$ ($a_1 = b_1 \oplus c_4 b_2 = 0$).

Jiný příklad. Je třeba zjednodušit lineární generátor ze třídy $\{1, 255\}$ zadaný charakteristickým mnohočlenem $f(X) = X^8 \oplus X^6 \oplus X^5 \oplus X^3 \oplus 1$. Generátor lze snadno

Tabulka 5.

Minimalizace $f(X) = X^8 \oplus X^6 \oplus X^5 \oplus X^3 \oplus 1$

	X^7	X^6	X^5	X^4	X^3	X^2	X	1
c			1					1
b		1						

realizovat osmičlenným registrem se 4 zpětnými vazbami, tj. se třemi sčítačkami mod 2 (např. maticí typu (*C*) nebo (*B*)). Jedno zjednodušené řešení je v tab. 5 a schéma vyžadující jen dvou sčítaček mod 2 je totožné se schématem z [7] (str. 151) nalezeném intuitivně. Kromě právě uvedeného tvaru lze psát okamžitě jeho duální protějšek: $c_6 = b_5 = b_0 = 1$.

Tabulka 6.

Přehled nejkratších nerozložitelných a primitivních mnohočlenů $f(X)$ a příslušných minimálních smíšených matic

Stupeň mnoho-členu n	Mnohočlen $f(X)$	Počet zpětných vazeb	Nenulové prvky c, b matice $[T]$	Počet sčítaček mod 2	Počet minimál-ních obvodů
2	$X^2 \oplus X \oplus 1$	2	$c_1 b_0$	1	2
3	$X^3 \oplus X \oplus 1$ $X^3 \oplus X^2 \oplus 1$	2	$c_1 b_0$ $c_2 b_0$	1	4
4	$X^4 \oplus X \oplus 1$ $X^4 \oplus X^3 \oplus 1$	2	$c_1 b_0$ $c_3 b_0$	1	4
5	$X^5 \oplus X^2 \oplus 1$ $X^5 \oplus X^3 \oplus 1$	2	$c_2 b_0$ $c_3 b_0$	1	4
6	$X^6 \oplus X \oplus 1$ $X^6 \oplus X^5 \oplus 1$	2	$c_1 b_0$ $c_5 b_0$	1	4
7	$X^7 \oplus X^3 \oplus 1$ $X^7 \oplus X^4 \oplus 1$	2	$c_3 b_0$ $c_4 b_0$	1	4
8	$X^8 \oplus X^6 \oplus X^5 \oplus X^3 \oplus 1$ $X^8 \oplus X^5 \oplus X^3 \oplus X^2 \oplus 1$ $X^8 \oplus X^5 \oplus X^3 \oplus X \oplus 1$ $X^8 \oplus X^6 \oplus X^5 \oplus X^2 \oplus 1$ $X^8 \oplus X^6 \oplus X^3 \oplus X^2 \oplus 1$ $X^8 \oplus X^7 \oplus X^3 \oplus X^2 \oplus 1$ $X^8 \oplus X^7 \oplus X^6 \oplus X \oplus 1$ $X^8 \oplus X^7 \oplus X^2 \oplus X \oplus 1$	3	$c_6 b_5 b_0$ $c_5 b_3 b_2$; $c_5 b_3 c_2$ $c_5 b_3 c_1$; $c_5 b_3 b_1$ $c_6 c_5 b_2$ $c_6 c_3 b_2$ $c_7 b_3 b_0$ $c_7 c_6 b_1$ $c_7 c_2 b_1$; $c_7 b_2 b_0$	2	22
9	$X^9 \oplus X^4 \oplus 1$ $X^9 \oplus X^5 \oplus 1$	2	$c_4 b_0$ $c_5 b_0$	1	4
10	$X^{10} \oplus X^3 \oplus 1$ $X^{10} \oplus X^7 \oplus 1$	2	$c_3 b_0$ $c_7 b_0$	1	4
11	$X^{11} \oplus X^2 \oplus 1$ $X^{11} \oplus X^9 \oplus 1$	2	$c_2 b_0$ $c_9 b_0$	1	4

Tabulka 6 (*pokračování*).

Stupeň mnohočlenu n	Mnohočlen $f(X)$	Počet zpětných vazeb	Nenulové prvky c, b matice $[T]$	Počet sčítaček mod 2	Počet minimálních obvodů
12	$X^{12} \oplus X^9 \oplus X^3 \oplus X^2 \oplus 1$ $X^{12} \oplus X^9 \oplus X^8 \oplus X^5 \oplus 1$ $X^{12} \oplus X^8 \oplus X^5 \oplus X \oplus 1$ $X^{12} \oplus X^{10} \oplus X^2 \oplus X \oplus 1$	3	$c_9 b_3 c_2$; $c_9 b_3 b_2$ $c_9 b_8 b_0$ $c_8 b_5 b_0$ $c_{10} b_2 c_1$; $c_{10} b_2 b_1$	2	12
13	$X^{13} \oplus X^{12} \oplus X^{10} \oplus X^9 \oplus 1$ $X^{13} \oplus X^8 \oplus X^6 \oplus X \oplus 1$ $X^{13} \oplus X^7 \oplus X^6 \oplus X^5 \oplus 1$ $X^{13} \oplus X^{10} \oplus X^3 \oplus X \oplus 1$ $X^{13} \oplus X^{10} \oplus X^5 \oplus X^2 \oplus 1$ $X^{13} \oplus X^{10} \oplus X^8 \oplus X^5 \oplus 1$ $X^{13} \oplus X^8 \oplus X^5 \oplus X^3 \oplus 1$ $X^{13} \oplus X^{10} \oplus X^4 \oplus X \oplus 1$ $X^{13} \oplus X^9 \oplus X^4 \oplus X^3 \oplus 1$ $X^{13} \oplus X^{10} \oplus X^5 \oplus X^3 \oplus 1$ $X^{13} \oplus X^{10} \oplus X^8 \oplus X^3 \oplus 1$ $X^{13} \oplus X^{11} \oplus X^2 \oplus X \oplus 1$ $X^{13} \oplus X^9 \oplus X^7 \oplus X^3 \oplus 1$ $X^{13} \oplus X^7 \oplus X^6 \oplus X^3 \oplus 1$ $X^{13} \oplus X^{12} \oplus X^4 \oplus X^3 \oplus 1$ $X^{13} \oplus X^{11} \oplus X^7 \oplus X^2 \oplus 1$ $X^{13} \oplus X^{11} \oplus X^6 \oplus X^2 \oplus 1$ $X^{13} \oplus X^{12} \oplus X^{11} \oplus X \oplus 1$ $X^{13} \oplus X^{12} \oplus X^2 \oplus X \oplus 1$ $X^{13} \oplus X^{12} \oplus X^7 \oplus X^6 \oplus 1$ $X^{13} \oplus X^7 \oplus X^6 \oplus X \oplus 1$	3	$c_{12} b_{10} b_0$ $c_8 b_6 b_0$ $c_7 b_6 c_5$; $c_7 b_6 b_5$ $c_{10} b_3 c_1$; $c_{10} b_3 b_1$ $c_{10} b_5 b_0$ $c_{10} b_8 b_0$ $c_8 b_5 c_3$; $c_8 b_5 b_3$ $c_{10} b_4 b_0$ $c_9 b_4 c_3$; $c_9 b_4 b_3$ $c_{10} c_5 b_3$ $c_{10} c_8 b_3$ $c_{11} b_2 c_1$; $c_{11} b_2 b_1$ $c_9 b_7 c_3$; $c_9 b_7 b_3$ $c_7 b_6 c_3$; $c_7 b_6 b_3$ $c_{12} b_4 b_0$ $c_{11} c_7 b_2$ $c_{11} c_6 b_2$ $c_{12} c_{11} b_1$ $c_{12} b_2 b_0$; $c_{12} c_2 b_1$ $c_{12} b_7 b_0$ $c_7 b_6 c_1$; $c_7 b_6 b_1$	2	60
14	$X^{14} \oplus X^{11} \oplus X^4 \oplus X^3 \oplus 1$ $X^{14} \oplus X^{11} \oplus X^{10} \oplus X^3 \oplus 1$ $X^{14} \oplus X^9 \oplus X^8 \oplus X^3 \oplus 1$ $X^{14} \oplus X^{11} \oplus X^4 \oplus X \oplus 1$ $X^{14} \oplus X^{12} \oplus X^2 \oplus X \oplus 1$ $X^{14} \oplus X^{13} \oplus X^{12} \oplus X^2 \oplus 1$ $X^{14} \oplus X^{13} \oplus X^3 \oplus X^2 \oplus 1$ $X^{14} \oplus X^{12} \oplus X^5 \oplus X^2 \oplus 1$ $X^{14} \oplus X^{12} \oplus X^9 \oplus X^2 \oplus 1$ $X^{14} \oplus X^{12} \oplus X^7 \oplus X^5 \oplus 1$ $X^{14} \oplus X^9 \oplus X^7 \oplus X^2 \oplus 1$	3	$c_{11} c_4 b_3$ $c_{11} c_{10} b_3$ $c_9 b_8 b_0$ $c_{11} b_4 b_0$ $c_{12} b_2 c_1$; $c_{12} b_2 b_1$ $c_{13} c_{12} b_2$ $c_{13} b_3 b_0$ $c_{12} c_5 b_2$ $c_{12} c_9 b_2$ $c_{12} b_7 b_0$ $c_9 b_7 b_0$	2	24
15	$X^{15} \oplus X \oplus 1$ $X^{15} \oplus X^{14} \oplus 1$	2	$c_1 b_0$ $c_{14} b_0$	1	4

Tabulka 6 (*pokračování*).

Stupeň mnohočlenu n	Mnohočlen $f(X)$	Počet zpětných vazeb	Nenulové prvky c, b matice $[T]$	Počet sčítaček mod 2	Počet minimálních obvodů
16	$X^{16} \oplus X^{10} \oplus X^7 \oplus X^6 \oplus 1$ $X^{16} \oplus X^{10} \oplus X^9 \oplus X^6 \oplus 1$ $X^{16} \oplus X^{10} \oplus X^7 \oplus X \oplus 1$ $X^{16} \oplus X^{13} \oplus X^9 \oplus X^6 \oplus 1$ $X^{16} \oplus X^{14} \oplus X^{13} \oplus X^{11} \oplus 1$ $X^{16} \oplus X^{11} \oplus X^6 \oplus X^5 \oplus 1$ $X^{16} \oplus X^{11} \oplus X^{10} \oplus X^5 \oplus 1$ $X^{16} \oplus X^{15} \oplus X^{12} \oplus X \oplus 1$ $X^{16} \oplus X^{15} \oplus X^4 \oplus X \oplus 1$ $X^{16} \oplus X^9 \oplus X^7 \oplus X^5 \oplus 1$ $X^{16} \oplus X^9 \oplus X^7 \oplus X^4 \oplus 1$ $X^{16} \oplus X^{14} \oplus X^9 \oplus X^7 \oplus 1$ $X^{16} \oplus X^9 \oplus X^7 \oplus X^2 \oplus 1$	3	$c_{10}c_7b_6$ $c_{10}c_9b_6$ $c_{10}b_7b_0$ $c_{13}b_9b_0$ $c_{14}b_{13}b_0$ $c_{11}c_6b_5$ $c_{11}c_{10}b_5$ $c_{15}c_{12}b_1$ $c_{15}c_4b_1$ $c_9b_7c_5$; $c_9b_7b_5$ $c_9b_7c_4$; $c_9b_7b_4$ $c_{14}b_9b_0$ $c_9b_7c_2$; $c_9b_7b_2$	2	32
17	$X^{17} \oplus X^3 \oplus 1$ $X^{17} \oplus X^{14} \oplus 1$	2	c_3b_0 $c_{14}b_0$	1	4
18	$X^{18} \oplus X^7 \oplus 1$ $X^{18} \oplus X^{11} \oplus 1$	2	c_7b_0 $c_{11}b_0$	1	4

Protože nejširšího použití v praxi dosáhly lineární generátory maximálních posloupností, jsou v tab. 6 uvedeny všechny tyto generátory pro $n = 2$ až 18. Kromě $n = 8, 12, 13, 14$ a 16 existují vždy nerozložitelné a primitivní mnohočleny délky 2 realizovatelné jedinou sčítačkou mod 2; v ostatních případech bylo nutno probrat všechny mnohočleny délky 4 a pokusit se o zjednodušení ($p = 3$), neboť pro nerozložitelné a primitivní mnohočleny délky 6 nelze dosáhnout $p < 4$. V tab. 6 jsou uvedeny jen výsledné minimální tvary s počtem potřebných zpětných vazeb a sčítaček mod 2 (vždy jen jeden z duálních), příslušnou strukturní matici a schéma si čtenář může sestrojit sám.

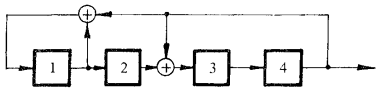
6. DALŠÍ APLIKACE

Metoda syntézy a minimalizace sice platí obecně, ale příklady byly voleny úmyslně jen z oboru lineárních generátorů maximálních posloupností. Pro další aplikace použijeme některých výsledků z [1].

Je-li mnohočlen $f(X)$ nerozložitelný ale primitivní, realizuje nějaký lineární generátor ze třídy $\{k_1, k_2, \ldots, k_r\}$, $r > 2$, jehož příslušná matice $[T]$ udává strukturu

schématu a složitost. Např. $f(X) = X^4 \oplus X^3 \oplus X^2 \oplus X \oplus 1$, který je nerozložitelný a neprimitivní, definuje lineární generátor ze třídy $\{1, 5, 5, 5\}$. Je vidět, že k jeho realizaci je potřeba tří sčítaček mod 2. Minimalizací lze však nalézt strukturní matici $[T]$ s prvky např. $b_0 = c_3 = b_2 = 1$ (schéma na obr. 4) – počet sčítaček mod 2 je roven dvěma.

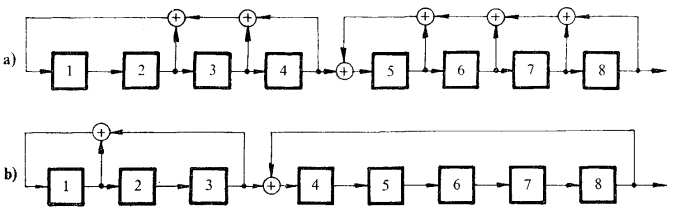
Rozložitelné mnohočleny jsou složitějším výrazem. Je třeba rozlišovat mezi rozložitelnými mnohočleny, jejichž součinitele jsou vzájemně nesoudělné (pro ně platí,



Obr. 4. Minimální schéma lineárního generátoru ze třídy $\{1, 5, 5, 5\}$.

že příslušný lineární generátor lze realizovat kaskádním spojením lineárních obvodů odpovídajících jednotlivým součinitelům, což vždy nemusí vést k minimálnímu tvaru) a mezi rozložitelnými mnohočleny se soudělnými nebo opakujícími se součiniteli.

Uveďme hned dva příklady. První z nich se týká zjednodušení lineárního generátoru zadaného charakteristickým mnohočlenem $f(X) = (X^4 \oplus X^2 \oplus X \oplus 1) . (X^4 \oplus X^3 \oplus X^2 X \oplus 1) = X^8 \oplus X^7 \oplus X^5 \oplus X^3 \oplus X^2 \oplus 1$, tvořený součinem

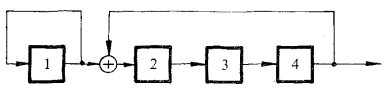


Obr. 5. Zjednodušení lineárního generátoru daného rozložitelným mnohočlenem a) s použitím kaskádního spojení a b) skutečně minimální.

dvou nesoudělných a nerozložitelných mnohočlenů. Použijeme-li pravidla o kaskádním spojení, dostaneme lineární generátor na obr. 5a. Sestrojením smíšené matice k mnohočlenu $X^4 \oplus X^3 \oplus X^2 \oplus X \oplus 1$ (obr. 4) se počet sčítaček mod 2 zmenší na 5. Realizací mnohočlenu $X^8 \oplus X^7 \oplus X^5 \oplus X^3 \oplus X^2 \oplus 1$ strukturní maticí typu (C) nebo (B) se ještě dále zmenší počet sčítaček mod 2 o jednu. Jeden z minimálních tvarů (nebudeme celý postup podrobně popisovat) je na obr. 5b; schéma vyžaduje dvou sčítaček mod 2 a navíc je vyjádřeno jiným kaskádním spojením dvou lineárních generátorů: $f_1(X) = X^3 + X^2 + 1$ a $f_2(X) = X^5 + 1$, přičemž $f(X) = f_1(X) f_2(X)$.

Druhou úlohou je minimalizace lineárního generátoru ze třídy $\{1, 1, 2, 3, 3, 6\}$ daného mnohočlenem $f(X) = (X \oplus 1)^2 (X^2 \oplus X \oplus 1) = X^4 \oplus X^3 \oplus X \oplus 1$. Původně by vyžadoval dvě sčítačky mod 2, po minimalizaci (obr. 6) je potřeba jen jedné a opět struktura obvodu prozrazuje rozklad původního mnohočlenu na $(X \oplus 1)(X^3 \oplus 1)$.

Smíšená matice $[T]$ může mít i některé speciální tvary (kromě typu (C) a (B)). Analyzujme matici $[T]$ s těmito prvky c a b : $c_{n-r} = 1$, $c_{n-j} = 0$ pro $j > r$, $r < n$; $b_{n-s} = 1$, $b_{n-i} = 0$ pro $i > s$, $r + s = n - d$, $d > 0$ a $b_0 = 1$ a označme ji $[T_{rs}]$. Schéma takto definovaného lineárního generátoru má soustředěny sčítačky mod 2 pro prvních r zpožďovacích obvodů vně posuvného registru (obr. 1), pro posledních



Obr. 6. Minimální lineární generátor ze třídy $\{1, 1, 2, 3, 3, 6\}$.

s zpožďovacích obvodů uvnitř posuvného registru (obr. 2) a $(r + 1)$-ní až $(r + d)$-tý zpožďovací obvod neobsahuje zpětné vazby (protože $b_0 = 1$, je zaručena regularita strukturní matice $[T_{rs}]$ a obvod lineárního generátoru je charakteristický „nejdelší" zpětnou vazbou z n-tého zpožďovacího obvodu do prvního). Snadno dokážeme

Větu 3. *Charakteristický mnohočlen matice* $[T_{rs}]$ *je tvaru* $f(X) = 1 \oplus \oplus X^d f_1(X) f_2(X)$, *kde* $f_1(X) = X^r \oplus c_{n-1} X^{r-1} \oplus \ldots \oplus c_{n-r+1} X \oplus 1$, $f_2(X) = X^s \oplus \oplus b_{n-1} X^{s-1} \otimes \ldots \oplus b_{n-s+1} X \oplus 1$, $r + s + d = n$, $d > 0$.

K důkazu stačí použít věty 1b) a provést součin $f_1(X) f_2(X) = X^{n-d} \oplus \oplus (c_{n-1} \oplus b_{n-1}) X^{n-d-1} \oplus \ldots \oplus (c_{n-r+1} \oplus b_{n-s+1}) X \oplus 1$ s ohledem na definici prvků matice $[T_{rs}]$.

Věta 3 pak udává metodu zjednodušení lineárního generátoru speciálního typu, pro něž je $f(X) \oplus 1$ rozložitelný na $X^d f_1(X) f_2(X)$ a $p'_1 + p'_2 < p'$, kde p'_1 resp. p'_2 je délka $f_1(X)$ resp. $f_2(X)$ [8]. Jako příklad poslouží opět lineární generátor daný mnohočlenem $X^5 \oplus X^4 \oplus X^2 \oplus X \oplus 1 = 1 \oplus X(X \oplus 1)(X^3 \oplus 1)$. Výsledkem jsou dva minimální tvary (záměna $f_1(X)$ a $f_2(X)$ odpovídá duálním tvarům), ale další dva (obr. 3 a k němu duální) nelze takto získat, neboť jejich strukturní matice není tvaru $[T_{rs}]$. Obecně tedy strukturní matice $[T_{rs}]$ neposkytuje všechny varianty řešení, které lze získat sestrojením smíšené matice typu (BC) a dokonce v některých případech selže úplně (např. $f(X) = X^7 \oplus X^4 \oplus X^3 \oplus X^2 \oplus 1$ nelze uvedeným způsobem rozložit a přesto existuje minimální tvar např. $c_4 = b_3 = c_2 = 1$ vyžadující dvě sčítačky mod 2).

7. ZÁVĚR

V článku byla na příkladě analyzována činnost lineárních generátorů a formulována úloha syntézy z hlediska redukce zpětných vazeb. Zavedená smíšená matice typu

(*BC*) není jedinou, která splňuje podmínky úlohy. Ukazuje se však, že jiné typy matice nad polem dvou prvků, které zcela přirozeně mají předpoklady být vhodné pro syntézu a minimalizaci, nepřinášejí nové výsledky (např. matice s prvky $t_{ij} = 1$ pro $i = j + 1$, $j = 1, 2, \ldots, n - 1$, $t_{ij} = c_{n-j}$ a $t_{nj} = b_{n-j}$, $j = 1, 2, \ldots, n$, $t_{ij} = 0$ v ostatních případech, se redukuje buď na smíšenou matici typu (*BC*) nebo dokonce jen na matici typu (*B*) resp. (*C*)). Stále však zbývá provést důkladnější analýzu obecných matic nad polem dvou prvků (příp. nad obecným polem $\mathscr{P}$) a získat tak účinné algoritmy pro syntézu a minimalizaci lineárních generátorů.

Metody lineární algebry se zdají být vůbec vhodné pro syntézu a analýzu obecných lineárních automatů (některé dílčí výsledky jsou uvedeny v [1, 4, 7]). Řadu problémů může s úspěchem vyřešit i čistě algebraický přístup použitý např. v [2, 5]. Konečně výsledky z teorie lineárních automatů je třeba rozšířit i na nelineární automaty — — obecné konečné automaty.

Závěrem bych chtěl poděkovat dr. A. Perezovi a inž. J. Š. Haškovcovi za řadu podnětných připomínek a za diskusi kolem některých problémů.

(Došlo dne 15. dubna 1966.)

LITERATURA

[1] Elspas B.: The theory of autonomous linear sequential networks. IRE Trans. *CT-6* (1959, March), 1, 45—60.

[2] Gill A.: Analysis of linear sequential circuits by confluence sets. IEEE Trans. *EC*-13 (1964, June), 3, 226—231.

[3] Green J. H., San Soucie R. L.: An error correcting encoder and decoder of high efficiency. Proc. IRE *46*, 1741—1744.

[4] Gruder J. F., Perlman M.: A feedback shift-register scaler. IEEE Trans. Comm. and Electr. (1964, Nov.), 6, 745—752.

[5] Huffman D. A.: The synthesis of linear sequential coding networks. In Information Theory (ed. C. Cherry), Acad. Press, New York 1956.

[6] Мишина А. П., Проскуряков И. В.: Высшая алгебра (СМБ). Наука, Москва 1965.

[7] Peterson W. W.: Error-correcting codes. J. Wiley, 1961, New York (ruský překlad: Коды, исправляющие ошибки. Мир, Москва 1964).

[8] Roth H. H.: Linear binary shift register circuits utilizing a minimum number of mod-2 adders. IEEE Trans. *IT-11* (1965, April), 2, 215—220.

[9] Sholefield P.H.R.: Shift registers generating maximal length sequences. Electr. Technology *37* (1960, Oct.), 10, 389—394.

Synthesis and Minimization of Regular Linear Generators

JOSEF PUŽMAN

The paper deals with one method of synthesis and reduction of feedback loops of regular linear autonomous finite automata (regular linear binary shift register circuits – linear generators). The classes of these generators defined by the set of state cycles $\{k_1, k_2, \ldots, k_r\}$, where k_i, $i = 1, 2, \ldots, r$ are lengths of individual cycles and $\sum_{i=1}^{r} k_i = 2^n$ is a number of internal states (n is a number of delay circuits), are introduced; these classes are further divided into subclasses according to the output determined by the delay polynomial $F(D)$ of degree n and the associated polynomial $f(X) = X^n F(1/X)$ over the field of two elements, respectively. The regular linear generator itself is then defined by the field $\mathscr{P}$ of two elements, by the internal state space $\mathscr{S}$ and by the structural matrix $[T]$ over the field $\mathscr{P}$; the latter also uniquely determines the scheme of a linear circuit and its complexity. A synthesis consists in a construction of a structural matrix $[T]$ to a given polynomial $f(X)$ such that $f(X)$ is a characteristic and at the same time a minimal polynomial of $[T]$ and a number of nonzero elements of $[T]$ is the least. In the paper for the solution of such a problem certain matrices over the field of two elements are considered and an algorithm for their construction is described.

Ing. Josef Pužman, Výzkumný ústav spojů, Praha 5, Kobrova 2.