PROBLEMA CĂUTĂRII POLINOAMELOR IREDUCTIBILE ASUPRA EXTENSIEI CÂMPURILOR GALOIS

D. Bodean, Gh. Bodean
Universitatea Tehnică a Moldovei
dianabodean@gmail.com, gbodean@mail.md

Abstract. *In this work the solution of searching irreducible polynomials over extension Galois field is presented. The proposed algorithm is based on the trace generation and testing the subperiods resulted from factorization the field's Euler indicator. Algorithm complexity is NP-polynomial. The searching results shows that the expected number of irreducible polynomials differ from the expected one known.*

Cuvinte-cheie: *Galois field extention, irreducible polynomial.*

I. Introducere

Câmpurile Galois au un spectru larg de aplicare în sistemele de achiziție şi procesare a datelor. Dintre domeniile de aplicație evidențiem criptografia, codurile corectoare de erori, diagnosticarea şi testarea aparatajului electronic. Specific, în practică, sunt aplicate extensiile câmpurilor Galois $\mathbf{GF}^k(2^m)$ generate de polinoamele ireductibile $g(z)=\sum_{i=0}^{k} g_i z^i$ cu coeficienții g_i asupra câmpurilor $\mathbf{GF}(2^m)$ generate de polinoamele ireductibile $p(x)=\sum_{i=0}^{m} p_i x^i$, unde $p_i \in \{0,1\}$ şi k, $m>1$. Conform definiției un polinom este ireductibil dacă nu poate fi prezentat prin produsul de polinoame, adică nu poate fi factorizat. În general, problema factorizării (e.g. fundamentală în aritmetica numerelor întregi) polinoamelor este *NP*-complexă. În acest articol va fi prezentată o metodă de căutare a polinoamelor generatoare de câmpuri extinse $\mathbf{GF}^k(2^m)$, bazată pe calculul traseelor şi factorizării indicatorului Euler. Algoritmul, ce realizează metoda, este hard-implementabil ceea ce permite accelerarea procedeului de căutare a polinoamelor ireductibile asupra extensiei câmpurilor Galois.

I. Formularea problemei

Notăm prin

$$g(z)=\sum_{i=0}^{k} g_i z^i \,, \tag{1}$$

unde $g_i \in \mathbf{GF}(2^m)/p(x)$, polinomul generator al elementelor câmpului Galois $\mathbf{GF}^k(2^m)$, unde $p(x)=\sum_{i=0}^{m} p_i x^i$ şi $p_i \in \mathbf{GF}(2)=\{0,1\}$. În virtutea dualismului polinoamelor, restricționăm analiza cu polinoamele monice, pentru care $g_k=1$.

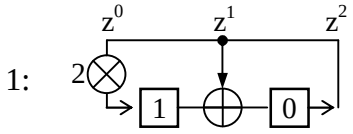
Modelul automat al polinomului (1) este registrul de deplasare cu reacție liniară, numit în continuare LFSR (Linear Feedback Shift Register). Legătura de reacție a LFSR-ului conține multiplicatoare modulare şi sumatoare XOR (bit-cu-bit).

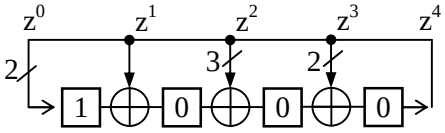
Convenţional, un LFSR poate fi implementat cu sumatoare exterioare sau incluse. Pentru a păstra similaritatea cu operaţiile matematice (de divizare), vom accepta modelul LFSR cu sumatoare incluse. Unui polinom ireductibil g(z) îi corespunde un LFSR cu perioada maximă egală cu

$$T_{\max}=(2^m)^k-1 \qquad (2)$$

Viceversa, mărimea (2) poate fi folosită în calitate de test al ireductibilităţii polinomului (arbitrar) corespunzător g(*z*).

Exemplul 1. Fie câmpul trivial $\mathbf{GF}^2(2^2)$ şi polinomul generator $g(z)=2+z+z^2$ cu coeficienţii asupra $\mathbf{GF}(2^2)/1+x+x^2$. În fig.1, a) este prezentată diagrama LFSR-ului corespunzător şi stările acestuia într-o perioadă de timp egală cu 16 tacte. Uşor se observă că peste 15 tacte automatul simulat revine în starea iniţială, i.e. $<z^1, z^2>=<1, 0>$. Deoarece perioada LFSR-ului este egală cu cea maximă, $T=(2^2)^2-1=15$, rezultă că polinomul $g(z)=2+z+z^2$ este ireductibil.





1:			α^0				
2:	0	1	α^1	0	1	0	0
3:	2	1	α^2	0	0	1	0
4:	2	3	α^3	0	0	0	1
5:	1	1	α^4	2	1	3	2
6:	2	0	α^5	3	0	0	0
7:	0	2	α^6	0	3	0	0
8:	3	2	α^7	0	0	3	0
9:	3	1	α^8	0	0	0	3
10:	2	2	α^9	1	3	2	1
11:	3	0	α^{10}	2	0	0	0
12:	0	3	α^{11}	0	2	0	0
13:	1	3	α^{12}	0	0	2	0
14:	1	2	α^{13}	0	0	0	2
15:	3	3	α^{14}	3	2	1	3
16:	1	0	$\alpha^{15}\equiv\alpha^0$	1	0	0	0
	a)			*b*)			

Fig.1. Diagrame de stări ale automatelor: *a*) LFSR specificat de polinomul $g(z)= 2+ z+ z^2$;
b) LFSR specificat de polinomul $g(z)= 2+ z+ 3z^2+ 2z^3+ z^4$.

Fie $\boldsymbol{z}(i)=<z_1(i), z_2(i),\ldots, z_k(i)>$ şi $\boldsymbol{z}(j)=<z_1(j), z_2(j),\ldots, z_k(j)>$ stările LFSR-ului respectiv în momentele de timp (tactele) *i* şi *j* (*i*,*j*=0,1,…).

Remarca 1: Două stări, $\boldsymbol{z}(i)$ şi $\boldsymbol{z}(j)$, ale automatului LFSR sunt (reciproc) ***multiple*** dacă sunt multiple stările celulelor respective, $z_n(i)$ şi $z_n(j)$, unde n =1, 2, …, k.

Astfel, în *Exemplul* 1, starea iniţială $\alpha^0=\boldsymbol{z}(0)$ este multiplă cu starea $\alpha^5=\boldsymbol{z}(5)$ prin factorul 2 şi cu starea $\alpha^{10}=\boldsymbol{z}(3)$ multiplă prin factorul 3.

În exemplul următor perioada automatului LFSR, de asemenea, este egală cu 15, deşi parametrii câmpului sunt diferiţi de cei specificaţi pentru câmpul în exemplul precedent.

Exemplul 2. Fie câmpul $\mathbf{GF}^4(2^2)$ şi polinomul monic $g(z)=2+z+3z^2+2z^3+z^4$. Diagrama stărilor LFSR-ului corespunzător este prezentată în fig.1, b). Deoarece perioada automatului este mai mică decât cea maximă, egală cu $(z^2)^4-1=255$, rezultă că polinomul analizat este ***reductibil***, adică

factorizabil. Şi mai mult, perioada automatului este ***multiplă*** cu perioada maximă! (Această din urmă observare va avea un rol important în definitivarea algoritmului de testare a ireductibilității polinoamelor).

Remarca 2: A se observa că în *Exemplul* 2 periodicitatea stărilor reciproc multiple este egală cu 5.

II. Metoda de căutare a polinoamelor ireductibile

În metodele cunoscute de căutare a polinoamelor ireductibile asupra câmpurilor finite cel mai frecvent se aplică testul bazat pe calculul traseului. Însă pentru câmpul $\mathbf{GF}^k(2^m)$ noțiunea de traseu trebuie redefinită. În contextul stărilor reciproc multiple ale unui automat LFSR, introducem următoarea.

Definiție. Asupra extensiei câmpului Galois de polinoame traseul, *Tr*, este mulțimea multiplicatoarelor într-o perioadă.

Remarca 3. În cazul unei perioade maxime cardinalul traseului, #*Tr*, este egal cu 2^m-1. Vom unui acest traseu ***complet.***

Pentru un LFSR cu perioadă arbitrară (mai mică decât $T_{\max}$) această afirmație, în general, nu este justă.

Deci, testul de ireductibilitate pentru polinomul analizat, trebuie să verifice existența traseului complet. Pentru generarea traseului complet vor fi utile următoarele construcții (formale).

Indicatorul Euler este mărimea:

$$j = \frac{T_{\max}}{h} = \frac{(2^m)^k - 1}{2^m - 1}. \tag{3}$$

În (3) divizorul *h* specifică periodicitatea stărilor reciproc multiple, care se vor numi ***distincte***. Pentru două stări distincte *i* şi *j* are loc relația:

$$\forall n(z_n(i)=(f\cdot z_n(j)) \ \mathbf{mod}\ p(x)), \tag{4}$$

unde $f \in \mathbf{GF}(2^m)/\{0,1\}$ şi $n = 1, 2, ..., k$.

În momentul inițial de timp setăm *Tr*=0. Calculul traseului se reduce la "*colectarea*" multiplicatorilor *f* pentru *i*=fix şi $j=\overline{1,h}$, adică

$$Tr = Tr+f, \tag{5}$$

unde simbolul "+" specifică operația de înserare (reuniune).

În calitate de stare inițială fixă a automatului LFSR este rațional de a selecta α^0, şi anume, $\boldsymbol{z}(i=0)=<1,0,\ldots,0>$. Celelalte stări distincte se vor selecta la distanța φ, adică are loc

$$\boldsymbol{z}(i+1)= \boldsymbol{z}(i)^{\varphi} \ \mathbf{mod}\ p(x), \text{ unde } i = 0, 1, ..., \eta-1 \tag{6}$$

Dacă polinomul analizat g(*z*) este ireductibil asupra $\mathbf{GF}^k(2^m)$, atunci operația (6) va genera stări $\boldsymbol{z}^{(f)}(\cdot)=<f, 0, \ldots, 0>$, unde $f \in \{2,3,...,2^m-1\}$. În caz contrar, orice stare $\boldsymbol{z}(\cdot)$ diferită de $\boldsymbol{z}^{(f)}(\cdot)$, adică

$$\boldsymbol{z}(\cdot) \lessgtr \boldsymbol{z}^{(f)}(\cdot), \tag{7}$$

va specifica un polinom reductibil.

Astfel, construirea traseului *Tr* va consta în executarea iterativă a operațiilor (5), (6) şi (7), unde numărul maxim de iterații este delimitat de $\eta=2^m$-1. Dacă traseul este complet, atunci se trece la a doua etapă de testare a ireductibilității, şi anume la verificarea prezenței perioadelor incluse sau subperioadelor.

Subperioadele sunt specifice polinoamelor reductibile ale căror perioade *T* sunt multiple cu $T_{\max}$. Deci, problema căutării valorilor perioadelor se reduce la sarcina factorizării $T_{\max}$. În contextul

problemei fundamentale a aritmeticii, un număr întreg *I* poate fi reprezentat prin produsul puterilor numerelor prime:

$$I = \prod_{i=1}^{n} p_i^j , \tag{8}$$

unde *p* este un număr prim, iar j este un întreg pozitiv.

Fie *N* – numărul factorilor, inclusiv cu repetare, în descompunerea (8). Evident că $N \geq n$. Atunci testul ireductibilității trebuie să verifice până la

$$Q = \sum_{i=1}^{N-1} C_N^i = 2^N - 2 \tag{9}$$

combinații (*C*) ale factorilor dezvoltării:

$$j = \prod_{i=1}^{N} p_i , \tag{10}$$

unde unele numere prime *p* pot să se repete.

Remarca 4. Problema factorizării mărimii (10) poate fi rezolvată apriori. Practica arată că pentru valori mici ai parametrilor câmpului $k(\leq 8)$ și $m(\leq 8)$ numărul factorilor variază de la 2 până la 8.

Notăm prin $\mathbf{K}_N^i$ mulțimea de combinații din *N* a câte *i*, iar prin $\mathbf{F}_N^i$ - mulțimea produselor numerelor constitutive ale combinației mulțimii $\mathbf{K}_N^i$, unde $1 \leq i \leq N\text{-}1$.

Exemplul 3. Pentru parametrii (*k*, *m*)=(3, 4) indicatorul Euler φ este egal cu 273 care poate fi descompus în forma φ=3·7·13, unde numărul de factori *N* este egal cu 3. Sunt $C_3^1=3$ și $C_3^2=3$ combinații ale factorilor descompunerii, respectiv $\mathbf{K}_3^1=\{(3),(5),(13)\}$ cu $\mathbf{F}_3^1=\{3, 5, 13\}$ și $\mathbf{K}_3^2=\{(3,5), (3, 13), (5, 13)\}$ cu $\mathbf{F}_3^2=\{15, 39, 65\}$.

Poate fi demonstrat că pentru starea distinctă $\boldsymbol{z}(0)=\langle 1,0,\ldots,0\rangle$ este suficient de efectuat exponențierea

$$\boldsymbol{z}^{(f)}(0) = \boldsymbol{z}(0)^{f(\boldsymbol{F}_N^i)} \textbf{ mod } p(x) , \tag{11}$$

cu verificarea ulterioară a elementelor $\boldsymbol{z}_{(\cdot)}^{(f)}$ puterii (11):

$$1< z_1^{(f)} < 2^m \text{ and } \forall j,\ 1< j \leq k,\ z_j^{(f)} = 0. \tag{12}$$

Dacă condiția (12) este satisfăcută, atunci polinomul testat este reductibil, în caz contrar – ireductibil.

III. Algoritmul de căutare a polinoamelor ireductibile

Conform metodei descrise în compartimentul precedent, testul ireductibilității polinoamelor asupra extensiei câmpului Galois $\mathbf{GF}(2^m)$ constă în generarea traseului *Tr* cu testarea ulterioară a prezenței subperioadelor. În baza testului ireductibilității elaborat se propune următorul algoritm de căutare a polinoamelor ireductibile asupra $\mathbf{GF}^k(2^m)$, unde $k,m \geq 2$.

Algoritmul de căutare a polinoamelor ireductibile asupra $\mathbf{GF}^k(2^m)$, prezentat în pseudocod,

Input: *k*, *m* -- parametrii extensiei câmpului Galois;

$p(x) = \sum_{i=0}^{m} p_i x^i$ -- polinomul generator, $p_i \in \{0,1\}$;

$\mathbf{F}= \{ \mathbf{F}_N^1 , \mathbf{F}_N^2 , \ldots, \mathbf{F}_N^{N-1} \}$ -- setul produselor combinațiilor de numere prime ale factorizării indicatorului Euler

Output: *Irreducible* -- False sau True;

FeedBack -- legătura de reacție a automatului LFSR or coeficienții polinomului monic $g(z) = \sum_{i=0}^{k} g_i z^i$, unde g_k=1 și $g_i \in$ **GF**(2^m)={0,1,...,2^m-1}.

```
1:    begin Irreducible:= False; -- false pentru test
2:      for j in 1 to (2^m)^k-1 do -- pentru toate combinațiile posibile de coeficienți g(·)
3:        Generate FeebBack (j); -- generarea coeficienților g(·)
4:          if Significante (FeedBack(j)) then
5:            Compute (Tr(FeedBack(j))); -- calculul traseului
6:            if Tr(FeedBack(j)) is Complete then
7:                State:=<1, 0, ..., 0>; -- setarea stării distincte
8:                for i in 1 to N-1 do
9:                  Exp:=State^(F_N^i) mod p(x); -- exponențierea stării distincte
10:                 if (Exp[1]≠0 and Exp[1]≠1 and Exp[2...k-1]=0) then
11:                   Irreducible:=True; -- testul ireductibilității a trecut cu succes
12:                   Save(FeedBack(j)); -- salvarea polinomului ireductibil
13:                   Break; -- următorul FeedBack
                    end if;
                  end for;
              end if;
            end if;
        end for;
      end begin.
```

Câteva comentarii referitor la algoritm. În linia 4 este verificată semnificația coeficienților polinomului g(*z*). Dacă $g_0 \neq 0$ și pentru $1 \leq i < k$ există cel puțin un coeficient semnificativ, i.e. $g_i \neq 0$, atunci legătura de reacție *FeedBack* este acceptată semnificativă. În linia 6 se verifică dacă traseul *Tr* este complet, i.e. conține valorile de la 1 până la 2^m-1.

Complexitatea (asimptotică a) algoritmului este delimitată de mărimea:

$$O(m, k) \leq \#\mathbf{F}^{2^{m(k+1)-1}}, \tag{13}$$

unde #**F** este cardinalul mulțimii **F**.

În baza algoritmului elaborat a fost implementat softul de căutare a polinoamelor ireductibile asupra **GF**^{k}(2^m), interfața căruia este prezentată în figura 2. Rezultatele derulării softului sunt prezentate în Tabelul 1. Unele valori ai timpilor de căutare sunt prezentate în Tabelul 2. Programul s-a derulat pe un procesor Intel cu frecvența de executare a instrucțiunilor egală cu 2800 MHz.

Tabelul 1. Numărul polinoamelor ireductibile asupra câmpurilor Galois **GF**^{k}(2^m)

k \ *m*	2	3	4	5	6	7	8
2	4	18	64	300	864	5292	16384
3	12	144	576	9000	46656	592704	2211840
4	32	432	8192	120000	1658880	33191424	–
5	120	5400	96000	6480000	106920000	–	–
6	288	23328	1105920	166525200	–	–	–
7	1512	254016	18966528	–	–	–	–
8	4096	829440	–	–	–	–	–

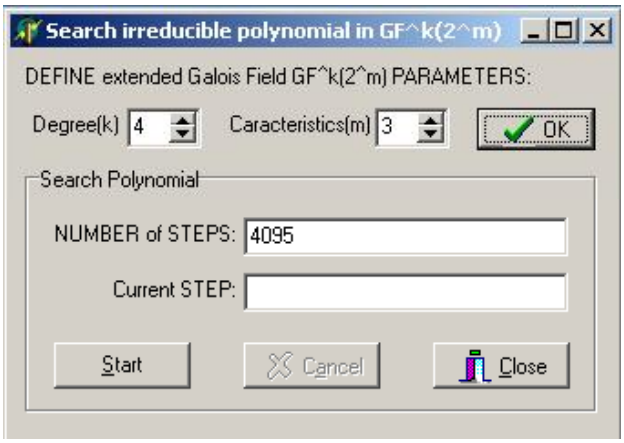


Fig.2. Interfața programului de căutare a polinoamelor ireductibile.

Tabelul 2. Parametrii temporali ai căutării polinoamelor ireductibile

k, *m*	Durata de cautare
7, 3	3 *min* 39 *sec*
3, 7	4 *min* 29 *sec*
8, 3	1 *h* 59 *min* 14 *sec*
3, 8	59 *min* 09 *sec*
5, 5	1 *h* 09 *min* 15 *sec*
5, 6	101 *h* 57 *min*
6, 5	137 *h* 52 *min* 52 *sec*

Remarca 5. În cazul când indicatorul Euler φ este un număr prim, instrucțiunea de repetare din linia 8 a Algoritmului nu se va executa. Sunt cazurile pentru valorile parametrilor (*k*, *m*) egale cu (2, 2), (2, 4), (2, 8), (3,3) şi (7, 7).

Din estimarea (13) şi din Tabelul 2 se observă că procedeul de căutare este de complexitate polinomială. Prin aceasta se explică faptul că pentru unele valori ai parametrilor *k* şi *m* încă n-au fost găsite valorile numărului de polinoame ireductibile (vezi celulele marcate cu simbolul "–" în tabelul 1).

Totodată, rezultatele experimentale arată că numărul polinoamelor ireductibile asupra extensiei câmpului Galois diferă de mărimea aşteptată, specificată în colorarul din [1].

IV. Concluzii

În lucrarea prezentă este soluționată problema căutării polinoamelor ireductibile asupra extensiei câmpurilor Galois. Soluția constă în calculul traseului şi testarea subperioadelor, rezultate din factorizarea indicatorului Euler. Complexitatea algoritmului de căutare este *NP*-polinomială. Ridicarea performanțelor instrumentarului soft de căutare poate fi realizată prin implementarea hard a operațiilor complexe, în particular, a exponențierii modulare.

Referințe

1. Lidl R., Niederreiter H. Finite Fields. – Cambridge University Press, 2003, 761 P.