CALCULUL MATRICEI-PRODUS A MULTIPLICATORLUI ASUPRA EXTENSIEI CÂMPULUI GALOIS

G. Bodean
Universitatea Tehnică a Moldovei

INTRODUCERE

În [1] a fost propusă şi analizată o metodă (tehnică) nouă de sintetizare (generare) a structurii (arhitecturii) multiplicatoarelor asupra câmpurilor Galois de caracteristica 2. Multiplicatoarele execută operaţia de înmulţire *modulară*, **modulo** $p(x)$, a două numere $A(x)$ şi $B(x)$ prezentate în forma standard polinomială: $A(x)=\sum_{i=0}^{m-1} a_i x^i$ şi $B(x)=\sum_{i=0}^{m-1} b_i x^i$, unde m este gradul polinomului generator $p(x)$, m= deg $p(x)$: $p(x)=\sum_{i=0}^{m} p_i x^i$, unde $a_i, b_i, p_i \in$ **GF**(2)={0,1}.

Dar necesităţile practicii impun proiectarea şi implementarea şi a multiplicatoarelor asupra *extensiilor* câmpurilor Galois **GF**^{k}(2^m) cu polinomul (generator) primitiv $g(x)=\sum_{i=0}^{k} g_i x^i$ al cărui coeficienţi g_i aparţin **GF**(2^m). În acest caz produsul **modulo** $g(x)$:

$$C(x)=A(x)\cdot B(x) \ \mathbf{mod}\ g(x)=\sum_{i=0}^{k-1} c_i x^i , \qquad (1)$$

va fi calculat pentru numerele $A(x)=\sum_{i=0}^{k-1} a_i x^i$ şi $B(x)=\sum_{i=0}^{k-1} b_i x^i$, unde $a_i, b_i, c_i \in$ **GF**(2^m).

Relaţia (1) poate fi scrisă în forma matriceală şi anume:

$$\boldsymbol{Z}\cdot\boldsymbol{A}=\boldsymbol{C}, \qquad (2)$$

unde: **C**= $[c_0, c_1, \ldots, c_{k-1}]^T$ este vector-coloană a coeficienţilor produsului $C(x)$; **A**= $[a_0, a_1, \ldots, a_{k-1}]^T$ este vector-coloană a coeficienţilor polinomului $A(x)$; **Z**=[$\mathbf{z}_0$ $\mathbf{z}_1$ … $\mathbf{z}_{k-1}$] este o matrice de dimensiunea $k\times k$ cu coloanele $\mathbf{z}_i$, $i=\overline{0,k-1}$. Elementele $z_{i,j}$ ale coloanei $\mathbf{z}_i$ sunt funcţii liniare ale coeficienţilor $B(x)$, $j=\overline{0,k-1}$. Matricea **Z** se numeşte *matrice-produs* [2].

În lucrare este prezentată o tehnică generală de calcul al matricei-produs. Tehnica propusă este bazată pe emularea automatului liniar care constă dintr-un registru de deplasare cu legătură de reacţie liniară (LFSR). Poziţiile registrului iau valori din mulţimea **GF**^{k}(2^m)={0,1,…,2^{km}-1}, iar structura legăturii de reacţie este "dictată" de structura polinomului $g^{\perp}(x)$ *dual* cu polinomul $g(x)$.

1. CALCULUL PROPUS

Pentru generarea matricei-produs **Z** se execută următorii paşi:

1: de adus polinomul generator $g(x)$ la forma canonică;

2: de calculat polinomul $g^{\perp}(x)$ dual cu polinomul $g(x)$:

$$g^{\perp}(x)=x^k\, g(x^{-1}), \text{ unde } k=\deg g(x); \qquad (3)$$

3: de construit automatul LFSR corespunzător lui $g^{\perp}(x)$;

4: de stabilit relaţia dintre poziţiile x_i ale $g^{\perp}(x)$ şi coeficienţii b_i ai polinomului $B(x)$ precum urmează:

$$x_1 \mapsto b_{k-1},\ x_2 \mapsto b_{k-2},\ \ldots,\ x_k \mapsto b_0;$$

5: de executat

Algorithmul 1.
Intrare-Ieşire: automatul LFSR definit de polinomul $g^{\perp}(x)$
for j= 0 **to** k-1 **do**
 for i=0 **to** k-1 **do**
 { set 1 în poziţia registrului LFSR corespunzătoare lui b_i;
 înscrierea sumei coeficienţilor b_i semnificativi ca element z_{ij} al matricei **Z**;
 deplasarea (shift) registrului LFSR;
 }
end.

Remarca 1. Un polinom $g(x)$ este prezentat în forma canonică dacă g_k=1. În caz contrar, dacă $g_k\neq 1$, atunci polinomul $g(x)$ se reduce la forma canonică conform relaţiei:

$$g(x) = g_k^{-1} \sum_{i=0}^{k} g_i x^i \,. \qquad (4)$$

Să depanăm un exemplu.

***Exemplul* 1**. Considerăm înmulţirea asupra $\mathbf{GF}^4(2^2)$ cu $g(x)= 3x^4+ 2x+ 2$ asupra $\mathbf{GF}(2^2)=\{0, 1, 2, 3\}$ cu $p(x)= x^2+ x+ 1$. Definim tabelul de înmulţire **modulo** $p(x)$:

*	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

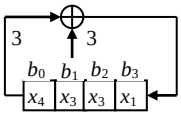
Găsim forma canonică a lui $g(x)$. Conform (4) avem:

$$g(x)= 3^{-1}(3x^4+ 2x+ 2)= x^4+3x+3. \qquad (5)$$

Conform (3) calculăm polinomul dual cu (5):

$$g^{\perp}(x) = x^4\left(\frac{1}{x^4}+\frac{3}{x}+3\right)=1+3x^3+3x^4\,. \qquad (6)$$

Acum depanăm algoritmul 1 pentru exemplul analizat. În fig.1 sunt prezentate etapele algoritmului 1 şi elementele z_{ij} rezultate, pe care le înscriem în matricea-produs:



i=0
1 0 0 0 → b_0
0 0 0 3 → $3b_3$
0 0 3 0 → $3b_2$
0 3 0 0 → $3b_1$

i=1
0 1 0 0 → b_1
1 0 0 3 → $b_0+ 3b_3$
0 0 3 3 → $3(b_2+ b_3)$
0 3 3 0 → $3(b_1+ b_2)$

i=2
0 0 1 0 → b_2
0 1 0 0 → b_1
1 0 0 3 → $b_0+ 3b_3$
0 0 3 3 → $3(b_2+ b_3)$

i=3
0 0 0 1 → b_3
0 0 1 0 → b_2
0 1 0 0 → b_1
1 0 0 3 → $b_0+ 3b_3$

Figura 1. Rezultatul depanării Algoritmului 1 pentru Exemplul 1.

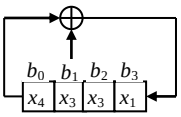
$$\mathbf{Z} = \begin{bmatrix} b_0 & 3b_3 & 3b_2 & 3b_1 \\ b_1 & b_0+3b_3 & 3(b_2+b_3) & 3(b_1+b_2) \\ b_2 & b_1 & b_0+3b_3 & 3(b_2+b_3) \\ b_3 & b_2 & b_1 & b_0+3b_3 \end{bmatrix}. \qquad (7)$$

Trebuie de remarcat că matricea (7) este aceiaşi ca şi în [3], dar calculată manual.

Remarca 2. Tehnica propusă de calcul al matricei-produs (2) este valabilă şi pentru cazul particular în care înmulţirea se execută asupra câmpului $\mathbf{GF}(2^m)$ cu polinomul generator asupra $\mathbf{GF}(2)$. Însă pentru acest caz, evident, din procedeu se va exclude pasul 1.

Demonstrativ în acest sens este următorul exemplu.

***Exemplul* 2**. Fie înmulţirea câmpul $\mathbf{GF}(2^4)$ cu polinomul generator $p(x)= x^4+x+1$. Dualul polinomului $p(x)$ este $p^{\perp}(x)= x^4+x^3+1$. Automatul LFSR corespunzător şi rezultatele depanării Algoritmului 1 sunt prezentate în fig. 2.



i=0
1 0 0 0 → b_0
0 0 0 1 → b_3
0 0 1 0 → b_2
0 1 0 0 → b_1

i=1
0 1 0 0 → b_1
1 0 0 1 → $b_0+ b_3$
0 0 1 1 → $b_2+ b_3$
0 1 1 0 → $b_1+ b_2$

i=2
0 0 1 0 → b_2
0 1 0 0 → b_1
1 0 0 1 → $b_0+ b_3$
0 0 1 1 → $b_2+ b_3$

i=3
0 0 0 1 → b_3
0 0 1 0 → b_2
0 1 0 0 → b_1
1 0 0 1 → $b_0+ b_3$

Figura 2. Rezultatul depanării Algoritmului 1 pentru Exemplul 2.

Rămâne numai de transcris expresiile rezultate (vezi coloana din dreapta) în liniile corespunzătoare ale matricei **Z** şi obţinem:

$$\mathbf{Z} = \begin{bmatrix} b_0 & b_3 & b_2 & b_1 \\ b_1 & b_0+b_3 & b_2+b_3 & b_1+b_2 \\ b_2 & b_1 & b_0+b_3 & b_2+b_3 \\ b_3 & b_2 & b_1 & b_0+b_3 \end{bmatrix},$$

care coincide cu rezultatul obţinut în [1].

***Exemplul* 3** - înmulţirea la constantă. În (1) înmulţirea la constanta $B=(b_0, b_1,\dots, b_{k-1})$, unde valorile $b_{(\cdot)}$ sunt fixate, se reduce la substituirea cu aceste valori în matricea-produs **Z**. Pentru exemplul 1 şi constanta $B= (2, 0, 1, 3)= 210_{10}$ matricea **Z** devine o *matrice-constantă* :

$$\mathbf{Z}=\begin{bmatrix} 2 & 3\cdot 3 & 3\cdot 1 & 3\cdot 0 \\ 0 & 2+3\cdot 3 & 3(1+3) & 3(0+1) \\ 1 & 0 & 2+3\cdot 3 & 3(1+3) \\ 3 & 1 & 0 & 2+3\cdot 3 \end{bmatrix}=\begin{bmatrix} 2 & 2 & 3 & 0 \\ 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & 1 \\ 3 & 1 & 0 & 0 \end{bmatrix}$$

şi înmulţirea factorului $A=(a_0, a_1, a_2, a_3)$ la constanta B este definită de:

$$\mathbf{C}=\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}=\begin{bmatrix} 2 & 2 & 3 & 0 \\ 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & 1 \\ 3 & 1 & 0 & 0 \end{bmatrix}\cdot\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}=\begin{bmatrix} 2a_0+2a_1+3a_2 \\ a_2+3a_3 \\ a_0+a_3 \\ 3a_0+a_1 \end{bmatrix}. \quad (8)$$

Precum rezultă din (8) se vor utiliza numai porţi XOR pentru implementarea multiplicatorului la constantă. În fig. 3 este prezentată bloc-diagrama multiplicatorului generată de structura (8).

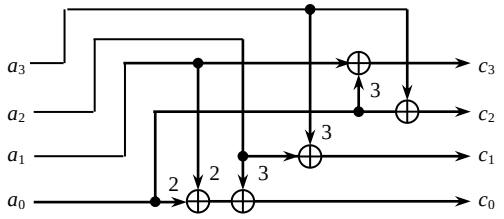


Figura 3. Block-diagrama multiplicatorului la constanta 210_{10} asupra $\mathbf{GF}^4(2^2)$.

Săgeţile din figura 3, marcate cu valorile factorilor din matricea (8), reprezintă multiplicatoare la constante asupra câmpului Galois $\mathbf{GF}(2^m)$, care pot fi generate prin tehnica descrisă în [1].

Remarca 3. Poate fi uşor verificat că multiplicatoarele la constantele 2 şi 3 vor conţine câte o poartă XOR cu două intrări.

2. PERFORMANŢA ŞI IMPLEMENTAREA

Performanţa unui multiplicator este estimată de două mărimi: complexitatea hard şi viteza (frecvenţa) de lucru. Eficienţa arhitecturii generate a multiplicatorului trebuie să fie comparată cu complexitatea multiplicatorului *exhaustiv*. Complexitatea unui astfel multiplicator este egală cu:

$$N_{\text{Full}}= (2k^2-3k+1)\oplus + (2k^2-k)\otimes, \quad (9)$$

unde $k=$ **deg** $g(x)$; simbolurile $\oplus$ şi $\otimes$ denotă respectiv poarta logică XOR şi multiplicatorul exhaustiv asupra $\mathbf{GF}(2^m)$.

În cazul când $g(x)$ este un trinom, atunci complexitatea hard a multiplicatorului asupra $\mathbf{GF}^k(2^m)$ este determinată de mărimea:

$$N(k)=(k-1)(k+1)\oplus+ k^2\otimes+ (k-1)\ \bar{\otimes}, \quad (10)$$

unde simbolul $\bar{\otimes}$ denotă multiplicatorul (optimizat) la constantă asupra $\mathbf{GF}(2^m)$ [1].

Comparând relaţiile (9) şi (10) se poate concluziona: *câştigul de la aplicarea tehnicii de calcul propuse este aproximativ de 2 ori*.

Frecvenţa de lucru a unui multiplicator este determinată de reţinerile semnalului în etajele arhitecturii. Pentru un multiplicator, generat de un *trinom*, timpul total de reţinere constituie mărimea:

$$T_{\bar{\otimes}}+T_{\otimes}+\left(1+\lceil\log_2 k\rceil\right)T_{\oplus}, \quad (11)$$

unde $T_{(\bullet)}$ – sunt timpii de reţinere (delay) în unităţile corespunzătoare.

Relaţiile (10) şi (11) sunt aplicate pentru estimarea apriori a performanţelor multiplicatoarelor. Tehnica propusă de sintetizare a arhitecturii multiplicatoarelor asupra câmpurilor Galois, inclusiv extinse, este simplu de implementat, iar rezultatul implementării este aplicaţia de generare a HDL-entităţilor, bune pentru utilizarea în sistemele de proiectare asistată de calculator.

Bibliografie

1. Bodean G. *Generarea multiplicatoarelor asupra câmpurilor Galois. – Meridian Ingineresc, no. 3, pp 14...21, 2006.*

2. Mastrovito E. *VLSI Architectures for Computations in Galois Fields. - PhD thesis, Linkoping University, Dept. Electrical Engineering, Linkoping, Sweden, 1991.*

3. Abrahamsson B. *Architectures for Multiplication in Galois Rings. Reg. nr: LiTH-ISY-EX-3549-2004.*