# GENERAREA MULTIPLICATOARELOR ASUPRA CÂMPURILOR GALOIS

***G. Bodean***
*Universitatea Tehnică a Moldovei*

## INTRODUCERE

Multiplicatoarele asupra câmpurilor finite sunt parte inerentă şi integrantă a dispozitivelor şi sistemelor contemporane de prelucrare a informaţiei.

Un câmp finit Galois de ordinul $2^m$ este definit de setul de elemente **GF**($2^m$)= {0,1,2,...,$2^m$-1} şi operaţiile *aditive* şi *multiplicative* **modulo** polinomul primitiv $p(x)=\sum_{i=0}^{m} p_i x^i$, unde $p_i \in$ **GF**(2)={0,1}; dimensiunea $m$ ia valori naturale. Pentru reprezentarea elementelor *extensiei* câmpului **GF**($2^m$) poate fi aleasă una din formele cunoscute: vectorială, polinomială, de putere, regulară etc. [1,2]. În tabelul 1 sunt prezentate variantele de formatare a elementelor câmpului **GF**($2^4$) cu polinomul $p(x)= x^4+x+1$.

**Tabelul 1**. Formele de reprezentare a elementelor câmpului **GF**($2^4$) cu $p(x)= x^4+x+1$.

| Vector $x^3x^2x^1x^0$ | Polinom $\sum_{i=0}^{m} a_i x^i,\ a_i \in \{0,1\}$ | De putere $\alpha^i$ | Regulară (număr zecimal) |
|---|---|---|---|
| 0000 | 0 | $\alpha^{-\infty}$ | 0 |
| 0001 | 1 | $\alpha^0$ | 1 |
| 0010 | $x$ | $\alpha^1$ | 2 |
| 0100 | $x^2$ | $\alpha^2$ | 4 |
| 1000 | $x^3$ | $\alpha^3$ | 8 |
| 0011 | $x$+1 | $\alpha^4$ | 3 |
| 0110 | $x^2+x$ | $\alpha^5$ | 6 |
| 1100 | $x^3+x^2$ | $\alpha^6$ | 12 |
| 1011 | $x^3+x+1$ | $\alpha^7$ | 11 |
| 0101 | $x^2+1$ | $\alpha^8$ | 5 |
| 1010 | $x^3+x$ | $\alpha^9$ | 10 |
| 0111 | $x^2+x+1$ | $\alpha^{10}$ | 7 |
| 1110 | $x^3+x^2+x$ | $\alpha^{11}$ | 14 |
| 1111 | $x^3+x^2+x+1$ | $\alpha^{12}$ | 15 |
| 1101 | $x^3+x^2+1$ | $\alpha^{13}$ | 13 |
| 1001 | $x^3+1$ | $\alpha^{14}$ | 9 |
| 0001 | 1 | $\alpha^0$ | 1 |
| ⋮ | ⋮ | ⋮ | ⋮ |

În câmpul Galois **GF**($2^m$) suma a două elemente (numere) $a$ şi $b$ este suma modulo 2 (XOR) bit cu bit (`bitwise`). Astfel:

$$c \equiv a+b = (a_0 \textbf{ xor } b_0,\ a_1 \textbf{ xor } b_1,\ \ldots,\ a_{m-1} \textbf{ xor } b_{m-1}) = (c_0, c_1, \ldots, c_{m-1}). \quad (1)$$

La înmulţirea a două numere se efectuează reducerea modulo $p(x)$. De exemplu, dacă numerele $a$ şi $b$ sunt reprezentate în forma vectorială, atunci poate fi aplicată metoda clasică (şcolară) de înmulţire. Metoda constă în deplasarea repetată a unuia din factori, adunarea modulo 2 a "deplasărilor" şi reducerea rezultatului modulo polinomul primitiv.

*Exemplul 1*. Fie **GF**($2^4$) cu $p(x)= x^4+x+1$. Din condiţia $p(x)\equiv 0$ rezultă $x^4\equiv x+1$, $x^5\equiv(x+1)\cdot x= x^2+x$, $x^6\equiv x^3+x^2$ etc. Înmulţirea clasică a două numere $a$=15=$1111_2$ şi $b$=9=$1001_2$ (reprezentate vectorial) este ilustrată în figura 1. Rezultatul obţinut este $c$=14= $1110_2$.

| | $x^6$ | $x^5$ | $x^4$ | $x^3$ | $x^2$ | $x^1$ | $x^0$ | |
|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 1 | 1 | 1 | |
| | | | × | 1 | 0 | 0 | 1 | |
| | | | | 1 | 0 | 0 | 1 | |
| + | | | 1 | 0 | 0 | 1 | | |
| | | 1 | 0 | 0 | 1 | | | |
| | 1 | 0 | 0 | 1 | | | | |
| | 1 | 1 | 1 | 0 | 1 | 1 | 1 | |
| | | | ↳ | 0 | 0 | 1 | 1 | -- $(x+1)\equiv x^4$ |
| | | ↳ | | 0 | 1 | 1 | 0 | -- $(x^2+x)\equiv x^5$ |
| | ↳ | | | 1 | 1 | 0 | 0 | -- $(x^3+x^2)\equiv x^6$ |
| | | | | 1 | 1 | 1 | 0 | → $x^3+x^2+x$ |

**Figura 1**. Înmulţirea clasică a două numere asupra **GF**($2^4$) cu $p(x)=x^4+x+1$.

Implementarea nemijlocită a schemei clasice de înmulţire asupra **GF**($2^m$) duce la o structură multietajată, cu alterarea etajelor de porţi logice SAU EXCLUSV (XOR) şi porţi logice ŞI (AND). Complexitatea multiplicatorului clasic va fi determinată de mărimea:

$$\#N= (2m^2-m)\ \text{AND} + (2m^2-3m+1)\ \text{XOR}. \quad (2)$$

Binaritatea m simbolurilor datelor prelucrate, de regulă, este multiplă cu 2 şi ia valori din seria 4, 8, 16, 32. Pe de altă parte, în dispozitivele sistemelor de telecomunicaţii – codare, decodare etc., sunt yeci de unităţi de înmulţire asupra câmpurilor finite. Deci, reducerea complexităţii hard, micşorarea timpului de reţinere a semnalelor sunt sarcini actuale şi stridente ale proiectării multiplicatoarelor asupra câmpurilor Galois extinse.

În acest articol este propusă şi analizată o metodă sistematică de generare a structurilor optimizate de înmulţire a numerelor, reprezentate în forma polinomială asupra câmpurilor Galois extinse. De asemenea, ca urmare a metodei propuse, este prezentat un algoritm simplu de generare a structurii optimale pentru multiplicatorul la constantă asupra **GF**($2^m$).

## 1. CALCULUL MATRICEAL AL MATRICEI-PRODUS

### *1.1. Matricea-produs*

În [3] a fost propusă o metodă de sintetizare a multiplicatoarelor, care permite generarea unei scheme optimizate de înmulţire polinomială asupra câmpurilor Galois **GF**($2^m$). Să reproducem succint esenţa metodei propuse.

Fie $A(x)=\sum_{i=0}^{m-1} a_i x^i$ şi $B(x)=\sum_{i=0}^{m-1} b_i x^i$ două polinoame, elemente ale câmpului **GF**($2^m$) cu polinomul primitiv $p(x)$ de gradul $m$, adică deg $p(x) = m$ . Produsul a două elemente:

$$C(x) = A(x)\cdot B(x) \ \mathbf{mod}\ p(x) = \sum_{i=0}^{m} c_i x^i , \quad (3)$$

precum a fost arătat în [3], poate fi scris în forma matriceală:

$$\mathbf{Z}\cdot\mathbf{A}=\mathbf{C}, \quad (4)$$

unde: $\mathbf{C}=[c_0, c_1, \ldots, c_{m-1}]^T$ este matricea(sau vector)-coloană a coeficienţilor produsului $C(x)$; $\mathbf{A}=[a_0, a_1, \ldots, a_{m-1}]^T$ este vector-coloană a coeficienţilor polinomului $A(x)$; $\mathbf{Z}=[\ \mathbf{z}_0\ \mathbf{z}_1\ \ldots\ \mathbf{z}_{m-1}]$ este o matrice de dimensiunea $m\times m$ cu coloanele $\mathbf{z}_i$, $i=\overline{0,m-1}$. Elementele $z_{i,k}$ ale coloanei $\mathbf{z}_i$ sunt funcţii liniare ale coeficienţilor $B(x)$, $k=\overline{0,m-1}$. Matricea $\mathbf{Z}$ se numeşte *matrice-produs* [3].

Relaţia matriceală (4) şi matricea produs $\mathbf{Z}$ se folosesc în proiectarea şi sintetizarea (generarea) structurii multiplicatorului asupra câmpului **GF**($2^m$) cu polinomul $p(x)$. Să analizăm un exemplu.

*Examplul 2*. Fie **GF**($2^4$) cu polinomul $p(x)=x^4+x+1$ şi două elemente arbitrare: $A(x)=a_0+a_1x+a_2x^2+a_3x^3$ şi $B(x)=b_0+b_1x+b_2x^2+b_3x^3$. Produsul:

$$C(x)= (a_0+a_1x+a_2x^2+a_3x^3)\cdot \cdot(b_0+b_1x+b_2x^2+b_3x^3)\ \mathbf{mod}\ (x^4+x+1), \quad (5)$$

după reducerea *modulo* $p(x)$, rezultă în relaţia:

$$\begin{aligned} C(x)\equiv\ & (a_3b_3 + a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3)x^3 + \\ & +( a_3b_3 + a_3b_2 + a_2b_3 + a_2b_0 + a_1b_1 + a_0b_2)x^2 + \\ & +(a_3b_2 + a_2b_3 + a_3b_1 + a_2b_2 + a_1b_0 + a_1b_3 + a_0b_1)x^1 + \\ & +( a_3b_1 + a_2b_2 + a_1b_3 + a_0b_0)\ x^0 = \\ & = (c_3, c_2, c_1, c_0). \end{aligned} \quad (6)$$

Relaţia (6) poate fi prezentată în următoarea formă de înmulţire matriceală (matrice la coloană):

$$\begin{bmatrix} b_0 & b_3 & b_2 & b_1 \\ b_1 & b_0+b_3 & b_2+b_3 & b_1+b_2 \\ b_2 & b_1 & b_0+b_3 & b_2+b_3 \\ b_3 & b_2 & b_1 & b_0+b_3 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix}. \quad (7)$$

Matricea-produs

$$Z = \begin{bmatrix} b_0 & b_3 & b_2 & b_1 \\ b_1 & b_0+b_3 & b_2+b_3 & b_1+b_2 \\ b_2 & b_1 & b_0+b_3 & b_2+b_3 \\ b_3 & b_2 & b_1 & b_0+b_3 \end{bmatrix} \quad (8)$$

defineşte aşa numita structură a arborelui binar de porţi XOR (BTR), iar relaţia (7) – structura multiplicatorului asupra câmpului **GF**($2^4$) cu $p(x)=x^4+x+1$ (figura 2). Multiplicatorul din figura 2 conţine porţi logice cu două intrări AND, reprezentate prin simbolul “ ⊐D– ”, şi porţi logice XOR, reprezentate prin simbolul “⊕”.

Complexitatea multiplicatorului din figura 2 este de 16 porţi AND şi 15 XOR. În general, complexitatea unui dispozitiv de înmulţire polinomială modulo un trinom este determinată de mărimea:

$$\#N= m^2\ \text{AND}+ (m^2-1)\ \text{XOR}. \quad (9)$$

În blocurile aritmetice asupra câmpurilor finite, de regulă, se operează cu date de binaritatea $m\geq 8$. Sintetizarea structurii multiplicatorului prin calculul direct al matricei $\mathbf{Z}$ (precum s-a procedat în Exemplul 2) pentru valori mari ale lui $m$ devine anevoioasă. De aceea, Mastrovito a apropus în [3] o metodă de calcul, bazată pe calculul unei matrice, numită *matrice redusă*. Însă, precum se menţionează în [4..10], metoda (schema) Mastrovito

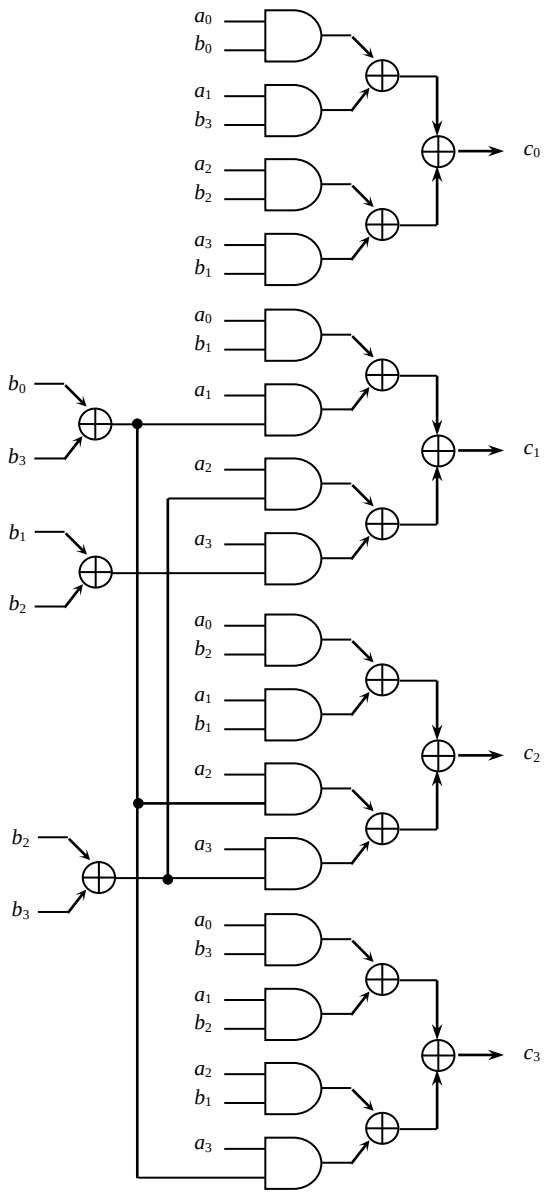


**Figura 2**. Multiplicatorul de tip paralel (asincron) asupra **GF**($2^4$) cu $p(x)=x^4+x+1$.

de calcul a matricei-produs este aplicabilă pentru valori moderate ale lui $m$ şi, odată cu creşterea lui $m$, devine complexă şi impracticabilă.

O altă metodă de calcul al matricei-produs este bazată pe transformarea Hankel-Toeplitz asupra câmpurilor Galois [11, 12]. Aplicarea transformatelor întotdeauna implică calcule "multietajate". Nici cazul analizat nu-i în afara acestei reguli. Deci, se impune necesitatea elaborării unei metode directe şi coincise de calcul al matricei-produs (8). În continuare se propune şi se analizează o metodă sistematică bazată pe un algoritm recurent de calcul matriceal al matricei-produs **Z**. Particularitatea esenţială a metodei propuse constă în aceea că se operează cu obiecte matematice binecunoscute în teoria automatelor.

## *1.2. Calculul matriceal*

Fie câmpul Galois **GF**($2^m$) cu polinomul primitiv $p(x)=\sum_{i=0}^{m} p_i x^i$. Notăm prin $q(x)=\sum_{i=0}^{m} q_i x^i$ *polinomul dual* cu $p(x)$, $q_i \in \{0,1\}$. De exemplu, dacă $p(x)= x^4+x+1$ atunci $q(x)= x^4+x^3+1$; dacă $p(x)= x^5+x^2+1$ atunci $q(x)= x^5+x^3+1$; dacă $p(x)= x^8+x^5+x^3+x^2+1$ atunci $q(x)= x^8+x^6+x^5+x^3+1$.

Asupra câmpului **GF**($2^m$) definim *matricea însoţitoare* (de tranziţii) a polinomului:

$$\mathbf{V}=\left[v_{kl}\right]=\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ q_m & q_{m-1} & q_{m-2} & \dots & q_1 \end{bmatrix}.$$

De axemplu, dacă $q(x)= x^4+x^3+1$ atunci matricea corespunzătoare **V** este:

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

Fie vectorii-coloane $\mathbf{a}= [a_0, a_1, \dots, a_{m-1}]^T$, $\mathbf{b}= [b_0, b_1, \dots, b_{m-1}]^T$ şi $\mathbf{c}= [c_0, c_1, \dots, c_{m-1}]^T$. Pentru prezentarea calculelor (în forma literală) introducem şi definim *operaţia de compoziţie* "$\circ$" a două coloane:

$$\mathbf{c}=\mathbf{a}\circ\mathbf{b}=\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{bmatrix}\circ\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{bmatrix}=\begin{bmatrix} a_0\circ b_0 \\ a_1\circ b_1 \\ \vdots \\ a_{m-1}\circ b_{m-1} \end{bmatrix},$$

unde $c_i = a_i \circ b_i$, $i=\overline{0,m-1}$.

Considerăm, în continuare, ecuaţia matriceală:

$$\mathbf{S}_i(t)=\mathbf{V}\cdot\mathbf{S}_i(t\text{-}1),\ t=1,2,\dots, \qquad (10)$$

şi compoziţia coloanelor:

$$\mathbf{z}_i(t)=\mathbf{S}_i(t)\circ\mathbf{b};\quad i=\overline{0,m-1}, \qquad (11)$$

unde: $\mathbf{b}=\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{m-1} \end{bmatrix}$, $b_{(.)}\in B(x)$; $\mathbf{S}_i(t)=\begin{bmatrix} s_0^{(t)} \\ s_1^{(t)} \\ \vdots \\ s_{m-1}^{(t)} \end{bmatrix}$ este matrice-coloană, componentele căreia sunt definite în modul următor:

$$s_k^{(t)}=\sum_{l=0}^{m-1} v_{kl}\, s_l^{(t-1)};\quad k=\overline{0,m-1}, \qquad (12)$$

şi, pentru $i$=0: $s_k^{(t)}=\begin{cases} 1, \text{ daca } k=t, \\ 0, \text{ in caz contrar}; \end{cases}$ $k=\overline{0,m-1}$.

Atunci, elementele $z_{ti}$ ale matricei-produs **Z** pot fi calculate în modul următor:

$$z_{ti}=\mathbf{1}^T\cdot\mathbf{z}_i(t)$$

ori

$$z_{ti}=\sum_{k-0}^{m-1} z_{i,k}^{(t)},\quad z_{i,k}^{(t)}\in\mathbf{z}_i(t);\quad i,t=\overline{0,m-1}, \qquad (13)$$

unde **1** este vector-coloană de unităţi, adică **1=** [1, 1, ..., 1]$^T$ or $\mathbf{1}^T$=<1 1 … 1>.

Suma şi înmulţirea în (12) şi (13) sunt respectiv operaţiile booleene XOR şi AND.

Pentru exemplul 2, cu $\mathbf{b}^T$=<$b_0$, $b_1$, $b_2$, $b_3$>, avem următorii paşi:

- $t$= 0, pentru $i=\overline{0,m-1}$: $\mathbf{S}_0(0)=\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$,

$$\mathbf{S}_1(0)=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}\cdot\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}=\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

$$\mathbf{S}_2(0)=\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix},\ \mathbf{S}_3(0)=\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

şi

$$\mathbf{z}_0(0)=\mathbf{S}_0(0)\circ\mathbf{b}=\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}\circ\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}=\begin{bmatrix} b_0 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

$$\mathbf{z}_1(0)=\mathbf{S}_1(0)\circ\mathbf{b}=\begin{bmatrix} 0 \\ 0 \\ 0 \\ b_3 \end{bmatrix},$$

$$\mathbf{z}_2(0)=\mathbf{S}_2(0)\circ\mathbf{b}=\begin{bmatrix} 0 \\ 0 \\ b_2 \\ 0 \end{bmatrix},\ \mathbf{z}_3(0)=\mathbf{S}_3(0)\circ\mathbf{b}=\begin{bmatrix} 0 \\ b_1 \\ 0 \\ 0 \end{bmatrix},$$

$$z_{00}=\mathbf{1}^T\cdot\mathbf{z}_0(0)=<1\ \ 1\ \ 1\ \ 1>\cdot\begin{bmatrix} b_0 \\ 0 \\ 0 \\ 0 \end{bmatrix}=b_0,$$

$$z_{01}=\mathbf{1}^T\cdot\mathbf{z}_1(0)=b_3,$$

$$z_{02}=\mathbf{1}^T\cdot\mathbf{z}_2(0)=b_2,\ z_{03}=\mathbf{1}^T\cdot\mathbf{z}_3(0)=b_1.$$

- Următorul pas, $t$=1, pentru $i=\overline{0,m-1}$ calculăm:

$$\mathbf{S}_0(1)=\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix},$$

$$\mathbf{S}_1(1)=\mathbf{V}\cdot\mathbf{S}_0(1)=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}\cdot\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}=\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

$$\mathbf{S}_2(1)=\begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix},\ \mathbf{S}_3(1)=\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix},$$

$$\mathbf{z}_0(1)=\mathbf{S}_0(1)\circ\mathbf{b}=\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}\circ\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}=\begin{bmatrix} 0 \\ b_1 \\ 0 \\ 0 \end{bmatrix},$$

$$\mathbf{z}_1(1)=\mathbf{S}_1(1)\circ\mathbf{b}=\begin{bmatrix} b_0 \\ 0 \\ 0 \\ b_3 \end{bmatrix},$$

$$\mathbf{z}_2(1)=\mathbf{S}_2(1)\circ\mathbf{b}=\begin{bmatrix} 0 \\ 0 \\ b_2 \\ b_3 \end{bmatrix},$$

$$\mathbf{z}_3(1)=\mathbf{S}_3(1)\circ\mathbf{b}=\begin{bmatrix}0\\b_1\\b_2\\0\end{bmatrix},$$

$$z_{10}=\mathbf{1}^T\cdot\mathbf{z}_0(1)=<1\quad 1\quad 1\quad 1>\cdot\begin{bmatrix}0\\b_1\\0\\0\end{bmatrix}=b_1,$$

$z_{11}=\mathbf{1}^T\cdot\mathbf{z}_1(1)=b_0+b_3$,
$z_{12}=\mathbf{1}^T\cdot\mathbf{z}_2(1)=b_2+b_3$,
$z_{13}=\mathbf{1}^T\cdot\mathbf{z}_3(1)=b_1+b_2$.

- Mai departe, $t$=2 şi pentru $i=\overline{0,m-1}$, avem:

$$\mathbf{S}_0(2)=\begin{bmatrix}0\\0\\1\\0\end{bmatrix},$$

$$\mathbf{S}_1(2)=\mathbf{T}\cdot\mathbf{S}_0(2)=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0\end{bmatrix}\cdot\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},$$

$$\mathbf{S}_2(2)=\begin{bmatrix}1\\0\\0\\1\end{bmatrix},\ \mathbf{S}_3(2)=\begin{bmatrix}0\\0\\1\\1\end{bmatrix},$$

$$\mathbf{z}_0(2)=\mathbf{S}_0(2)\circ\mathbf{b}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}\cdot\begin{bmatrix}b_0\\b_1\\b_2\\b_3\end{bmatrix}=\begin{bmatrix}0\\0\\b_2\\0\end{bmatrix},$$

$$\mathbf{z}_1(2)=\mathbf{S}_1(2)\circ\mathbf{b}=\begin{bmatrix}0\\b_1\\0\\0\end{bmatrix},$$

$$\mathbf{z}_2(2)=\mathbf{S}_2(2)\circ\mathbf{b}=\begin{bmatrix}b_0\\0\\0\\b_3\end{bmatrix},$$

$$\mathbf{z}_3(2)=\mathbf{S}_3(2)\circ\mathbf{b}=\begin{bmatrix}0\\0\\b_2\\b_3\end{bmatrix},$$

$$z_{20}=\mathbf{1}^T\cdot\mathbf{z}_0(2)=<1\quad 1\quad 1\quad 1>\cdot\begin{bmatrix}0\\0\\b_2\\0\end{bmatrix}=b_2,$$

$z_{21}=\mathbf{1}^T\cdot\mathbf{z}_1(2)=b_1$,
$z_{22}=\mathbf{1}^T\cdot\mathbf{z}_2(2)=b_0+b_3$,
$z_{23}=\mathbf{1}^T\cdot\mathbf{z}_3(2)=b_2+b_3$ ;

- $t$=3, pentru $i=\overline{0,m-1}$: $\mathbf{S}_0(3)=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}$,

$$\mathbf{S}_1(3)=\mathbf{T}\cdot\mathbf{S}_0(3)=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&1&0&0\end{bmatrix}\cdot\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix},$$

$$\mathbf{S}_2(3)=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ \mathbf{S}_3(3)=\begin{bmatrix}1\\0\\0\\1\end{bmatrix},$$

$$\mathbf{z}_0(3)=\mathbf{S}_0(3)\circ\mathbf{b}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}\cdot\begin{bmatrix}b_0\\b_1\\b_2\\b_3\end{bmatrix}=\begin{bmatrix}0\\0\\0\\b_3\end{bmatrix},$$

$$\mathbf{z}_1(3)=\mathbf{S}_1(3)\circ\mathbf{b}=\begin{bmatrix}0\\0\\b_2\\0\end{bmatrix},\ \mathbf{z}_2(3)=\mathbf{S}_2(3)\circ\mathbf{b}=\begin{bmatrix}0\\b_1\\0\\0\end{bmatrix},$$

$$\mathbf{z}_3(3)=\mathbf{S}_3(3)\circ\mathbf{b}=\begin{bmatrix}b_0\\0\\0\\b_3\end{bmatrix},$$

$$z_{30}=\mathbf{1}^T\cdot\mathbf{z}_0(3)=<1\quad 1\quad 1\quad 1>\cdot\begin{bmatrix}0\\0\\0\\b_3\end{bmatrix}=b_3,$$

$z_{31} = \mathbf{1}^T \cdot \mathbf{z}_1(3) = b_2$,

$z_{32} = \mathbf{1}^T \cdot \mathbf{z}_2(3) = b_1$, $z_{33} = \mathbf{1}^T \cdot \mathbf{z}_3(3) = b_0 + b_3$.

Deci, matricea-produs **Z** asupra **GF**($2^4$) cu $p(x)= x^4+x+1$ este:

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

exact aceiaşi ca şi (8).

Metoda elaborată este lesne de implementat. Respectivul program a fost realizat. Pentru cazul, important pentru practică, şi anume, multiplicatorul asupra **GF**($2^8$) cu $p(x)= x^8+x^5+x^3+x^2+1$ şi $q(x)= x^8+x^6+x^5+x^3+1$, a fost generată matricea-produs, prezentată în figura 3. Multiplicatorul corespunzător este de complexitatea 64 porţi (cu 2 intrări) AND şi 44 porţi 2-XOR (fără optimizare!).

Astfel, metoda recurentă propusă, bazată pe calculul matriceal (10),…, (13), generează matricea-produs **Z** pentru ecuaţia (4). Tot odată, ecuaţia (4) este "sarcina pentru proiectare" a structurii optimale a multiplicatorului asupra câmpului Galois **GF**($2^m$) cu polinomul generator $p(x) = \sum_{i=0}^{m} p_i x^i$, $p_i \in \{0,1\}$.

Însă din punct de vedere practic, mai frecventă este necesitatea proiectării multiplicatorului la constantă, adică a dispozitivului de înmulţire la constantă asupra **GF**($2^m$).

## 2. MULTIPLICATORUL LA CONSTANTĂ

Generarea structurii multiplicatorului la constantă este un caz particular al metodei descrise anterior. În (7) înmulţirea la constanta $B=(b_0, b_1, \ldots, b_{m-1})$, unde coeficienţii $b_{(\cdot)}$ au valori fixe, pur şi simplu va însemna substituţia acestor valori în matricea-produs **Z**. Pentru exemplul 2, dacă constanta este $B=(0,1,0,1)$, atunci matricea **Z** devine o matrice binară (constantă):

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

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

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

$$\mathbf{C} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} =$$

$$= \begin{bmatrix} a_1 + a_3 \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_2 + a_3 \\ a_0 + a_2 + a_3 \end{bmatrix}. \qquad (14)$$

In figura 4 este prezentată bloc-diagrama multiplicatorului la constantă, proiectată în conformitate cu relaţia (14). Numai porţi logice cu 2 intrări XOR sunt utilizate pentru implementarea proiectului. Precum poate fi observat, numărul de porţi 2XOR este egal cu 8 (de comparat cu multiplicatorul din figura 2).

Structura multiplicatorului la constantă poate fi definită printr-o, aşa numita, (0,1)-matrice de forma:

$$\mathbf{Z} = \begin{bmatrix} b_0 & b_7 & b_6 & b_5 & b_4 & b_3+b_7 & b_2+b_6+b_7 & b_1+b_5+b_6+b_7 \\ b_1 & b_0 & b_7 & b_6 & b_5 & b_4 & b_3+b_7 & b_2+b_6+b_7 \\ b_2 & b_1+b_7 & b_0+b_6 & b_5+b_7 & b_4+b_6 & b_3+b_5+b_7 & b_2+b_4+b_6+b_7 & b_1+b_3+b_5+b_6 \\ b_3 & b_2+b_7 & b_1+b_6+b_7 & b_0+b_5+b_6 & b_4+b_5+b_7 & b_3+b_4+b_6+b_7 & b_2+b_3+b_5+b_6 & b_1+b_2+b_4+b_5 \\ b_4 & b_3+b_7 & b_2+b_6+b_7 & b_1+b_5+b_6+b_7 & b_0+b_4+b_5+b_6 & b_3+b_4+b_5 & b_2+b_3+b_4 & b_1+b_2+b_3+b_7 \\ b_5 & b_4 & b_3+b_7 & b_2+b_6+b_7 & b_1+b_5+b_6+b_7 & b_0+b_4+b_5+b_6 & b_3+b_4+b_5 & b_2+b_3+b_4 \\ b_6 & b_5 & b_4 & b_3+b_7 & b_2+b_6+b_7 & b_1+b_5+b_6+b_7 & b_0+b_4+b_5+b_6 & b_3+b_4+b_5 \\ b_7 & b_6 & b_5 & b_4 & b_3+b_7 & b_2+b_6+b_7 & b_1+b_5+b_6+b_7 & b_0+b_4+b_5+b_6 \end{bmatrix}$$

**Figura 3**. Matricea-produs asupra GF($2^8$) cu $p(x)= x^8+x^5+x^3+x^2+1$.

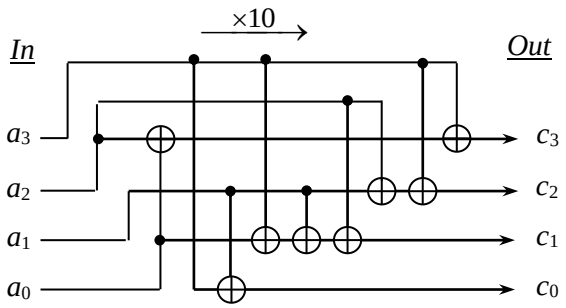


**Figura 4**. Bloc-diagrama multiplicatorului la constanta 10 asupra **GF**($2^4$) cu $p(x)=x^4+x+1$.

$$\Delta = [\delta_{ij}], \text{ unde } \delta_{ij} \in \{0,1\};\ i, j = \overline{0, m-1}. \qquad (15)$$

În (15) elementele $\delta_{ij}$ sunt egale cu 1 dacă există conexiune dintre intrarea $a_i$ şi ieşirea $c_j$ în structura multiplicatorului la constantă. Pentru bloc-diagrama prezentată în figura 4 matricea $\Delta$ este:

$$\Delta_{10} = \begin{array}{c} \\ a_0 \\ a_1 \\ a_2 \\ a_3 \end{array} \begin{array}{c} \begin{array}{cccc} c_0 & c_1 & c_2 & c_3 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \end{array}.$$

Structurile multiplicatorului la constantă şi a matricei $\Delta$ sunt izomorfe.

Poate oare fi generată matricea $\Delta$ implicit? Analiza problemei puse a arătat că matricea $\Delta$ poate fi generată fără aplicarea calculului matriceal prezentat în compartimentul precedent. Ca rezultat avem următorul algoritm:

**Algoritm:** Generarea matricei $\Delta$ asupra câmpului Galois **GF**($2^m$) cu

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

**Intrare**: Constanta $D(x)= (d_0, d_1,..., d_{m-1})$
$d_i \in \{0,1\}$;
Polinomul $p(x)= ( p_0, p_1,..., p_m)$
**Ieşire**: Matricea $\Delta=[\delta_{ij}]_{m\times m}$
**Auxiliar**: Repositoriu $R= (r_0, r_1,..., r_m)$,
$r_i \in \{0,1\}$;
Pas 1: $R \leftarrow (d_0, d_1,..., d_{m-1}, 0)$
Pas 2: **for** $i = 0$ **to** $m$-1 **do**
Pas 3: **for** $j = 0$ **to** $m$-1 **do**
Pas 4: $\delta_{ij} \leftarrow 0$ {iniţializarea matricei $\Delta$}
Pas 5: **for** $i = 0$ **to** $m$-1 **do**
Pas 6: **for** $j = 0$ **to** $m$-1 **do**
Pas 7: $\delta_{ij} \leftarrow \delta_{ij} \oplus r_j$ {bitwise XORing}
Pas 8: *ShiftLeft*( $R$) {Multiply $R$ by 2}
Pas 9: **if** $r_m = 1$ **then** $R \leftarrow R \oplus p(x)$

*Exemplul 3*. În figura 5 sunt prezentate matricele $\Delta$ generate de algoritm pentru multiplicatoarele la constantă asupra **GF**($2^3$) cu $p(x)= x^3+x+1$. Precum poate fi observat, multiplicatoarele la 3 şi 6 sunt celea mai complexe – numărul de porţi 2XOR este egal cu 4. Pe de altă parte, complexitatea multiplicatorului universal este egală cu 9 porţi AND şi 8 porţi XOR !

Complexitatea medie a multiplicatoarelor la constantă asupra **GF**($2^3$) este egală cu 2,5. În tabelul 2 sunt prezentate caracteristicile multiplicatoarelor universale şi la constantă asupra **GF**($2^m$) cu trinom. Din tabelul 2 rezultă un câştig considerabil al cheltuielilor hard.

$$\Delta_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ \Delta_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix},\ \Delta_3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},\ \Delta_4 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix},$$

0 1 4 2 -- numărul de porţi 2-XOR

$$\Delta_5 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},\ \Delta_6 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix},\ \Delta_7 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

Numărul de porţi 2-XOR: 1 4 3

**Figura 5**. Matricele $\Delta$ şi complexitatea hard a multiplicatoarelor la constantă modulo $x^3+x+1$.

**Tabelul 2**. Analiza comparativă a multiplicatoarelor asupra **GF**($2^m$) cu trinom.

| | Multiplicatoare la constantă | | | | Multiplcatoare universale | |
|---|---|---|---|---|---|---|
| | Polinom primitiv, $p(x)$ | Complexitatea medie, Nr. porţi 2-XOR | Cel mai complex multiplicator la constant (MCM), constantele | Complexitatea MCM, Nr. porţi 2-XOR | Complexitatea | |
| | | | | | Porţi 2-AND | Porţi 2-XOR |
| 1 | $x^3+x+1$ | 2.5 | 3, 6 | 4 | 9 | 8 |
| 2 | $x^4+x+1$ | 4.8 | 7 | 9 | 16 | 15 |
| 3 | $x^5+x^2+1$ | 8.2 | 14, 28 | 14 | 25 | 24 |
| 4 | $x^6+x+1$ | 12.5 | 23, 46 | 23 | 36 | 35 |
| 5 | $x^7+x+1$ | 17.8 | 47 | 33 | 49 | 48 |
| 6 | $x^9+x^4+1$ | 31.6 | 248, 496 | 52 | 81 | 80 |
| 7 | $x^{10}+x^3+1$ | 40.1 | 127 | 69 | 100 | 99 |
| 8 | $x^{11}+x^2+1$ | 49.5 | 830, 1660 | 86 | 121 | 120 |
| 9 | $x^{15}+x+1$ | 95.5 | 10943, 21886 | 170 | 225 | 224 |

## CONCLUZII

În acest articol este propusă şi analizată o metodă recurentă de generare a matricei-produs a multiplicatorului asupra câmpului Galois **GF**($2^m$) cu polinomul primitiv $p(x)$. Metoda este bazată pe un calcul matriceal, cu implicarea matricei însoţitoare a polinomului dual cu $p(x)$. În rezultatul calculului se obţine matricea-produs, elementele căreia sunt funcţii liniare ale coeficienţilor unuia din factori. Multiplicatorul, corespunzător matricei, conţine un număr optimal de porţi logice AND şi XOR.

Un caz particular, dar important pentru practică, sunt multiplicatoarele la constantă. În lucrare este propus şi analizat un algoritm simplu de generare a structurilor multiplicatoarelor la constantă. Multiplicatoarele generate au o structură optimală şi conţin numai porţi logice XOR. Complexitatea hard a multiplicatoarelor la constantă este în medie de 4..5 ori mai mică decât a multiplicatorului general.

Metoda matriceală de calcul a matricei-produs este o generalizare teoretică a schemei Mastrovito de sintetizare a structurii multiplicatorului şi poate fi foarte utilă în proiectarea asistată de calculator a dispozitivelor aritmeticii câmpurilor finite.

### *Bibliografie*


1. **Lidl R. and Niederreiter H.** *Finite fields. - Cambridge, University Press, 1997.*
2. **MacWilliams F.J and Sloane N.J.A.** *The theory of Error-Correcting Codes. – North-Holland, 1978.*
3. **Mastrovito E. D.** *VLSI Architectures for Computations in Galois Fields. - PhD thesis, Linkoping University, Dept. Electrical Engineering, Linkoping, Sweden, 1991.*
4. **Paar C.** *Efficient VLSI Architectures for Bit-Parallel Computation in Galois Field. - PhD thesis, Institutes for Experimental Mathematics, University of Essen, Essen, Germany, June, 1994.*
5. **Paar C. and Rosner M.** *Comparison of arithmetic architectures for Reed-Solomon decoders in reconfigurable hardware. - IEEE Transactions on Computers, vol. 41, no. 8, pp. 219..224, 1997.*
6. **Paar C., Fleischmann P. and Roelse P.** *Efficient Multiplier Architectures for Galois Fields GF($2^{4n}$). - IEEE Transactions on Computers, vol. 47, no. 2, pp. 162..170, 1998.*
7. **Sunar B. and Koc C. K.** *Mastrovito multiplier for all trinomials. - IEEE Transactions on Computers, vol. 48, no. 5, pp. 522..527, 1999.*
8. **Halbutogulları A. and Koc C. K**. *Mastrovito Multiplier for General Irreducible Polynomials. - IEEE Transactions on Computers, vol. 49, no. 5, pp. 503 .. 518, 2000.*
9. **Rodriguez-Henriquez F. and Koc C. K.** *Parallel multipliers based on special irreducible pentanomials. - IEEE Transactions on Computers, vol. 52, no. 12, pp. 1535..1542, December 2003.*
10. **Reyhani-Masoleh A. and Hasan M. A.** *Low Complexity Bit Parallel Polynomial Basis Multiplication over GF($2^m$). - IEEE Transactions on Computers, vol. 53, no. 8, pp. 945..959, 2004.*
11. **Мутер В.М.** *Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат, 1990. - 288 с.*
12. **Zhang T. and Parhi K.K.** *Systematic Design of Original and Modified Mastrovito Multipliers for General Irreducible Polynomials. - IEEE Transactions on Computers, vol. 50, no. 7, pp. 734 .. 749, July 2001.*


***Aprobat spre publicare:05.04.2006***