PROBLEMA CĂUTĂRII MATROIDELOR UNIFORME

G. Bodean
Universitatea Tehnică a Moldovei

INTRODUCERE

În ultimul timp se observă o creştere a numărului de articole consacrate aplicării teoriei matroidelor în studiul codurilor corectoare de erori. Majoritatea lucrărilor au un caracter teoretic pronunţat şi se axează mai mult pe analiza proprietăţilor matroidelor. Această tratare unilaterală este cauzată de faptul că la formularea problemelor se presupune *deja cunoscută structura* codului corector şi cu acest cod se asociază matroidul respectiv. Apoi, în lucrare, cel mai frecvent se trece la soluţionarea problemelor legate cu reprezentarea matroidelor asupra câmpurilor finite, inclusiv şi Galois. Astfel, codul corector rămâne martor pasiv al naraţiunii expuse.

În lucrarea prezentă se încearcă distanţierea de la "algoritmul" tradiţional de tratare a matroidelor. Scopul lucrării este de a "impune" matroidele să joace un rol mai activ, creator în problematica generării codurilor corectoare şi, în special, a celor *non-binare*.

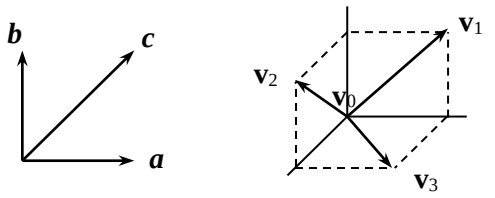
1. BREVIAR TEORETIC

Noţiunea de *matroid* a fost propusă de Hassler Whitney în [1] şi s-a format din cuvântul "matrix" prin adăugarea sufixului "-oid", astfel semnificând "asemănător unei matrice" sau "având forma matricei". Algebra matroidelor a fost introdusă cu scopul de a generaliza independenţa liniară în spaţiile vectoriale. Să analizăm un exemplu trivial.

Exemplul 1. fie matricea **M** asupra câmpului Galois **GF**(2):

$$\mathbf{M} = \begin{matrix} a & b & c \end{matrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}. \qquad (1)$$

Notăm prin $\mathbf{F}^n$ – spaţiul vectorial asupra câmpului finit **F**. Atunci coloanele matricei **M** pot fi interpretate ca o mulţime de vectori Q= {**a**, **b**, **c**} într-un spaţiu **W** bidimensional asupra **GF**(2); reprezentarea Q este ilustrată în figura 1, *a*. Din vectorii mulţimii Q pot fi construite baze (structuri ortogonale) în spaţiul 2-dimensional $\mathbf{GF}^2(2)$. Mulţimea acestor baze este {**ab**, **ac**, **bc**}.



a) *b*)

Figura 1. Spaţii vectoriale asupra **GF**(2).

Pe de altă parte matricea (1) poate fi interpretată ca o matrice generatoare a unui (n, k)-cod liniar $C_{\mathbf{M}}$ asupra câmpului **GF**(2), unde n şi k sunt respectiv lungimea şi dimensiunea (numărul de simboluri informaţionale) lui C. Pentru exemplul analizat, avem:

$$C_{\mathbf{M}} = \{000, 101, 011, 110\}. \qquad (2)$$

Remarcă. Codul $C_{\mathbf{M}}$ posedă numai proprietăţi detectoare, mai exact, este un cod cu control al parităţii.

Cu mulţimea (2) poate fi asociat setul de vectori $\mathbf{v}_0$, ...,$\mathbf{v}_3$ asupra **GF**(2), prezentat în figura 1, *b*. Vectorii (cuvintele de cod) **v** sunt combinaţii liniare dintre liniile matricei **M** care pot fi puse în forma:

$$\mathbf{v}=<v_1, \ldots, v_n>= \mathbf{x}\cdot \mathbf{M}, \qquad (3)$$

unde $\mathbf{x}= <x_1, \ldots, x_k>$, $x\in$ **GF**(2).

Relaţia (3) defineşte un set de ecuaţii liniare de forma $v_j = \sum_j m_{ij} x_j$, $m_{ij} \in \mathbf{M}$, $i=\overline{1,k}$, $j=\overline{1,n}$.

Dacă vom nota (marca) coloanele matricei **M** prin 1, 2 şi 3, atunci mulţimea $\mathcal{B}$ = {12, 13, 23} reliefează coeficienţii sistemelor de ecuaţii liniar-independente de rangul 2.

Această asociere dintre structurile ortogonale ale spaţiului vectorial asupra unui câmp finit şi sistemele de ecuaţii (mixte) liniar-independente asupra aceluiaşi câmp este chintesenţa teoriei matroidelor. Conform teoriei coloanele matricei (1) definesc un matroid liniar $\mathcal{M}$(**M**) [2].

În general, fie E mulţimea {1, …, n} de marcaje (indici) ale coloanelor matricei **M** de dimensiunea $k\times n$ asupra unui câmp finit **F** şi $\mathcal{B}$ – setul de submulţimi B din E. Atunci perechea (E, $\mathcal{B}$) defineşte un matroid dacă submulţimile B, $B\subset E$ şi

$B \in \mathcal{B}$, sunt liniar independente asupra **F,** ori, în mod axiomatic:

B1: pentru toate submulţimile A, $B_1 \subseteq E$, dacă $A \subseteq B_1$, $A \neq B_1$ şi $B_1 \in \mathcal{B}$, atunci $A \notin \mathcal{B}$.

B2: pentru orice bază B_1, B_2 şi oricare $x \in B_1$ se va găsi un astfel $y \in B_2$, încât $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Pentru exemplul 1 poate fi uşor verificată valabilitatea axiomelor B1 şi B2.

Fie E o mulţime de cardinalitatea n şi $\mathcal{B}$ – toate submulţimile din E de cardinalitatea k, $0 < k < n$. Atunci $\mathcal{B}$ este mulţimea (setul) bazelor matroidului pe E. Perechea $(E, \mathcal{B})$ se numeşte *matroid uniform* de rangul k şi se notează prin $U_{k,n}$ sau $U_k(n)$.

Matroidul $\mathcal{M}(\mathbf{M})$ din exemplul 1 este un matroid uniform de tipul $U_{2,3}$.

Încercarea de a extinde numărul de baze B de rangul 2 asupra **GF**(2) este sortită eşecului. Aici apare, aşa numita, problemă de *reprezentare* (sau *coordinatizare*) a matroidelor asupra câmpurilor finite. Conform definiţiei, un matroid $\mathcal{M}(\mathbf{M})$ cu matricea **M** asupra câmpului finit **F** se numeşte **F**-reprezenrabil, dacă există o astfel de funcţie $\phi: E \to \mathbf{F}^n$ care păstrează rangul, adică pentru orice submulţime $B \subset E$ are loc relaţia:

B independentă în $\mathcal{M}(\mathbf{M}) \Leftrightarrow$ mulţimea $\{\phi(b): b \in B\}$ este liniar independentă în $\mathbf{F}^n$.

Matricea **M** se numeşte **F**-reprezentarea matroidului $\mathcal{M}$ [3].

Problema coordinatizării matroidelor este centrală în teoria matroidelor [3]. Însă, din punct de vedere al generării codurilor corectoare de erori, interesează numai *matroidele uniforme*. Precum este bine ştiut [2, 3], nu orice matroid este reprezentabil asupra oricărui câmp. Matroidele reprezentabile asupra câmpurilor **GF**(2) şi **GF**(3) se numesc *binare* şi *ternare* respectiv. Matroidul uniform $U_{2,4}$ este ternar [2].

Exemplul 2. Matricea

$$\mathbf{N} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

reprezintă $U_{2,4}$ asupra **GF**(3). Codul asociat matricei **N** este un cod Hamming *non-binar*:

$$C_{\mathbf{N}} = \{0000, 1011, 0112, 1120\}. \quad (4)$$

Este uşor de observat că *distanţa minimă* $d_{\min}$ a codului $C_{\mathbf{N}}$ este egală cu 3. deci, capacitatea corectoare a codului (4) este egală cu 1.

Anume distanţa minimă este caracteristica definitorie în alegerea matroidelor uniforme în calitate de bază constructivă pentru generarea codurilor non-binare corectoare de t erori.

În practică, codarea şi decodarea codului $C_{\mathbf{N}}$ se realizează în modul următor. Sursa sistemului de comunicaţie conţine coderul, care implementează operaţia matriceală:

$$\mathbf{v} = \langle v_1, v_2, v_3, v_4 \rangle = \mathbf{x} \cdot \mathbf{N},$$

unde $\mathbf{x} = \langle x_1, x_2 \rangle$; $v, x \in \mathbf{GF}(3)$, sau

$$\begin{cases} 1: v_1 = x_1, \\ 2: v_2 = x_2, \\ 3: v_3 = x_1 + x_2, \\ 4: v_4 = x_1 + 2x_2. \end{cases} \quad (5)$$

Receptorul conţine decoderul care analizează setul de sisteme de ecuaţii liniare (5) şi determină dacă vectorul recepţionat $\mathbf{v}'$ conţine sau nu eroare. Calea trivială de a lua decizia constă în rezolvarea celor $C_4^2 = 6$ sisteme de 2 ecuaţii liniare independente: {1,2}, {1,3}, {1,4}, {2,3}, {2,4}, {3,4}, şi compararea rezultatelor obţinute. Conform [4] este suficient ca numărul soluţiilor identice să fie egal cu $C_{n-t}^k = C_3^2 = 3$. Însă, din considerente practice, prezintă interes numai matroidele asupra câmpurilor Galois cu caracteristica 2^m, unde $m = 1, 2, \ldots$ De aceea, în continuare va fi analizată problema reprezentării matroidelor asupra $\mathbf{GF}(2^m)$.

2. FORMULAREA PROBLEMEI

De ce căutarea matroidelor uniforme asupa unui câmp finit este o problemă complexă?

Fie câmpul $\mathrm{GF}(2^m)$. Căutarea candidaţilor în coloanele matroidului uniform $U_{k,n}$ se va face printre vectorii k-dimensionali ai spaţiului $\mathbf{GF}^k(2^m)$. Numărul total de vectori este egal cu 2^{km}.

Căutarea trivială constă în trierea tuturor combinaţiilor de n-vectori k-dimensionali. Complexitatea acestui procedeu este egală cu $C_{2^{mk}}^n$. Precum a fost demonstrat în [4], pentru construirea codului corector de t erori parametrii matroidului $U_{k,n}$ trebuie să satisfacă relaţia:

$$n \geq 2t + k. \quad (6)$$

Fie $t = k/2$, atunci $n = 2k$. În acest caz complexitatea trierii triviale este determinată de mărimea:

$$C_{2^{mk}}^{2k} = \frac{2^{mk}}{(2k)!\left(2^{mk}-2k\right)!}. \qquad (7)$$

În tabelul 1 sunt prezentate valorile mărimii (7) pentru unele valori *k* şi *m*. Analizând tabelul 1 devine clar de ce se spune că algoritmul de căutare a matroidelor are o *complexitate polinomială*.

Tabelul 1. Complexitatea căutării matroidelor uniforme $U_{k,2k}$ asupra **GF**(2^m).

k \ *m*	2	3	4	5	6
2	1820	635 376	1.75e8	4.55e10	1.17e13
3	7.5e7	2.43e13	6.53e18	1.72e24	4.51e29
4	4.1e14	1.95e24	8.44e33	3.62e43	1.56e53
5	3.34e23	3.93e38	4.43e53	4.99e68	5.61e83

Următorul pas constă în diminuarea complexităţii algoritmului de căutare. Este evident că din setul iniţial de vectori trebuie excluşi, în primul rând, vectorii liniar dependenţi.

Conform definiţiei vectorii **x**, **z**, ..., **y** din **W** vor fi liniar dependenţi dacă există astfel de numere α, β, ..., γ din **GF**(2^m), diferite (concomitent) de zero, încât:

$$\alpha\mathbf{x} + \beta\mathbf{y} + \ldots + \gamma\mathbf{z} = 0.$$

Se ştie că pentru a defini operaţiile aditive şi multiplicative în câmpul **GF**(2^m) este necesar de selectat un polinom ireductibil $p(x)$ de gradul m, adică **deg** $p(x) = m$, de forma:

$$p(x) = \sum_{i=0}^{m} p_i x^i, \text{ unde } p_i \in \mathbf{GF}(2).$$

Exemplul 3. Fie **GF**(2^2) cu $p(x) = 1 + x + x^2$ şi k=2. În spaţiul vectorial **GF**^{2}(2^2) avem următorul set de 16 vectori: S= {00, 01, 02, 0, 10, 11, 12, 13, 20, 21, 22, 23, 30, 31, 32, 33}. Luând în consideraţie regulile de înmulţire **mod** $p(x)$ în câmpul **GF**(2^2):

reprezentare polinomială şi numerică

•	0	1	*x*	*x*+1
0	0	0	0	0
1	0	1	*x*	*x*+1
x	0	*x*	*x*+1	1
x+1	0	*x*+1	1	*x*

sau

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

uşor se observă că vectorii 12, 23 şi 31 sunt liniar dependenţi. În rezultat, din cei 16 vectori iniţiali ai mulţimii S, vor rămâne numai 5 vectori liniar independenţi, şi anume, de exemplu, S^*={01, 10, 11, 12, 13}. Mulţimea S^* este, aşa numita, submulţime *ciclică* generată în extensia câmpului Galois **GF**^{2}(2^2).

Tabelul 2. Reprezentarea câmpului **GF**^{2}(2^2), $x^2 \equiv x+1$, $\alpha^2 \equiv 2\alpha+2$.

Coordonate dreptunghiulare			Coordonate polare	
Nr. crt.	Vector $\alpha^1\alpha^0$	Polinom $\sum_{i=0}^{k-1} \alpha^i z^i$	Gradul α^j	Logaritm $\log_\alpha \alpha^j$
0	00	0	$\alpha^{-\infty}$	$-\infty$
1	01	1	α^0	0
2	10	x	α^1	1
3	22	$2x+2$	α^2	2
4	13	$x+3$	α^3	3
5	12	$x+2$	α^4	4
6	02	2	α^5	5
7	20	$2x$	α^6	6
8	33	$3x+3$	α^7	7
9	21	$2x+1$	α^8	8
10	23	$2x+3$	α^9	9
11	03	3	α^{10}	10
12	30	$3x$	α^{11}	11
13	11	$x+1$	α^{12}	12
14	32	$3x+2$	α^{13}	13
15	31	$3x+1$	α^{14}	14
16	01	1	$\alpha^{15} \equiv \alpha^0$	0

În tabelul 2 sunt expuse reprezentările elementelor câmpului **GF**^{2}(2^2). La generarea elementelor în coordonate dreptunghiulare s-a folosit polinomul $g(z) = 1 + z + 3z^2$ ireductibil în câmpul **GF**^{2}(2^2).

În general, $g(z)$ numit *polinom generator al codului*, este dat de

$$g(z) = \sum_{i=0}^{k} g_i z^i, \quad z \in \mathbf{GF}\left(2^m\right). \qquad (8)$$

Vectorii din liniile 1..6 ale tabelului 2 sunt esenţa submulţimii ciclice. Are loc

Propoziţia 1: Într-un spaţiu vectorial k-dimensional asupra unui câmp Galois **GF**(2^m) numărul vectorilor liniar independenţi este determinat de mărimea:

$$\varphi(k,m) = \frac{2^{km}-1}{2^m-1}. \qquad (9)$$

Deoarece cardinalitatea submulţimii ciclice este determinată de mărimea (9), atunci complexitatea algoritmului de căutare (prin triere)

se va reduce de la mărimea (7) la mărimea $C^{2k}_{\varphi(k,m)}$. În tabelul 3 sunt prezentate unele valori ale acestei mărimi.

Tabelul 3. Complexitatea căutării matroidelor uniforme $U_{k,2k}$ în submulţimea ciclică.

k \ m	2	3	4	5	6
2	5	9	17	33	65
3	21	73	273	1057	4161
4	85	585	4369	33825	266305
5	341	4681	69905	1082401	17043521

Cu mărimea (9) este legată următoarea propoziţie care poate trezi interes din punct de vedere matematic:

Propoziţia 2: Numărul polinoamelor ireductibile $g(z)$ de gradul k asupra $\mathbf{GF}^k(2^m)$ este determinat de $\varphi(k, m)$.

Trebuie, însă, de menţionat că problema căutării polinoamelor $g(z)$ asupra câmpului Galois extins este şi ea *NP*-complexă!

Comparând tabelele 1 şi 3 stabilim că complexitatea căutării s-a micşorat considerabil. Însă rămâne excesiv de mare pentru valorile practice ale m şi k.

Deci, se impune de organizat o căutare mai "orientată pe obiect", mai consecventă. În acest context va fi util de căutat matroidele uniforme printre dezvoltările de puteri de forma α^0, α^1, α^2, …, α^{n-1} asupra unui câmp finit n-dimensional [5].

3. CĂUTAREA MATROIDELOR UNIFORME

În matematică sunt cunoscute mai multe structuri (obiecte) care pot fi acceptate în calitate de dezvoltări de puteri. Începem analiza cu aşa numitele *cicloclase* [6].

Fie α^i – un element primitiv al câmpului $\mathbf{GF}(2^m)$, unde $\alpha\neq 0$ şi i= 0, 1, …, 2^m-2. Atunci elementele α^i , α^{2i}, α^{4i} , ..., se numesc *conjugate,* iar mulţimea $\{\alpha^i , \alpha^{2i}, \alpha^{4i} , ...\}$ se numeşte *cicloclasă*. Elementul α se numeşte *generatorul* clasei.

Pentru căutarea matroidelor uniforme $U_{k,2k}$ vom utiliza cicloclasele de forma:

$$\mathcal{A}_n= \{\alpha, \alpha^2, \alpha^4, ..., \alpha^{2^{n-1}}\}, \qquad (10)$$

cu elementul generator $\alpha\in \mathbf{GF}^k(2^m)$.

Exemplul 4. Fie spaţiul vectorial (extensia câmpului) $\mathbf{GF}^2(2^2)$. Cicloclasele $\mathcal{A}_{n=4}$ generate asupra $\mathbf{GF}^2(2^2)$ sunt prezentate în tabelul 4.

Cicloclasele din tabelul 4 se numesc fundamentale. Cicloclasele generate de alte elemente ale câmpului $\mathbf{GF}^2(2^2)$ vor fi alăturate uneia din celea prezentate în tabelul 4.

Tabelul 4. Cicloclasele fundamentale $\mathcal{A}_{n=4}$ asupra $\mathbf{GF}^2(2^2)$.

Nr.crt.	$a= \log_\alpha \alpha^j$	Cicloclasa $\mathcal{A}_4$
1	2	$\alpha^1, \alpha^2, \alpha^4, \alpha^8$
2	4	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}\equiv\alpha^9$
3	6	$\alpha^5, \alpha^{10}, \alpha^{20}\equiv\alpha^5, \alpha^{10}$
4	8	$\alpha^7, \alpha^{14}, \alpha^{28}\equiv\alpha^{13}, \alpha^{26}\equiv\alpha^{11}$

Printre cicloclasele din tabelul 4 este una, şi anume, generată de elementul a= 4, care nu satisface proprietatea de independenţă. Acest tip de cicloclase le vom numi *reduse*. Poate fi uşor verificat că cicloclasele rămase reprezintă un matroid uniform $U_{2,4}$ asupra $\mathbf{GF}(2^2)$.

Deci, apare întrebarea: pentru n= 2k câte cicloclase fundamentale (fără celea reduse) asupra $\mathbf{GF}^k(2^m)$ pot fi generate?

Ca răspuns la această întrebare în tabelul 5 sunt prezentate valorile numărului de cicloclase fundamentale $N(\mathcal{A}_n)$ pentru n= 2k. În paranteze este indicat numărul de cicloclase reduse. Aceste valori au fost obţinute pe cale experimentală.

Tabelul 5. Numărul de cicloclase $N(\mathcal{A}_{2k})$ generate asupra $\mathbf{GF}^k(2^m)$

k \ m	2	3	4	5	6
2	4(1)	27(3)	104(1)	426(1)	1709(3)
3	12(3)	170(2)	1235(6)	10099(8)	80941(3)
4	34(4)	1116(1)	15725(4)	25881(10)	4146454(15)
5	106(7)	7453(8)	210088(10)	6908009(6)	222056530(18)

Comparând datele din tabelul 5 cu datele respective din tabelul 1 se observă că complexitatea căutării matroidelor uniforme $U_{k,2k}$ s-a micşorat drastic! Însă pentru valorile k şi m mari rămâne încă destul de mare. Mai adăugăm, pe lângă aceasta, faptul că nu toate cicloclasele fundamentale (fără celea reduse) reprezintă un matroid uniform. Într-adevăr, de exemplu, ciclocsa generată de elementul α^1: $\mathcal{A}_n$= {α^1: 010, α^2: 100, α^4: 031, α^8: 201, α^{16}: 022, α^{32}: 303}, asupra câmpului $\mathbf{GF}^3(2^2)$ cu $p(x)$= 1+ x+ x^2 şi $g(z)$= 1+ z+ $2z^2$+ $3z^3$ nu reprezintă

matroidul $U_{3,6}$, deoarece vectorii în submulţimile $\{\alpha^1, \alpha^4, \alpha^{16}\}$ şi $\{\alpha^2, \alpha^8, \alpha^{32}\}$ sunt liniar dependenţi. (Remarcăm faptul că proprietatea de independenţă se verifică prin calculul determinantului matricei respective!)

Enormitatea experimentelor efectuate pe calculator a demonstrat că:

în mulţimea cicloclaselor fundamentale $\mathcal{A}_n$ există cel puţin o cicloclasă care reprezintă un matroid uniform $U_{k,n}$ asupra câmpului GF(2^m).

Deci, calvarul căutărilor unui algoritm a adus la formularea "sentinţei": dezvoltările de puteri sunt keia succesului în optimizarea procesului de generare a matroidelor uniforme asupra câmpurilor Galois extinse.

Întrebare: poate sunt şi alte tipuri de dezvoltări de puteri care ar sta la baza generării matroidelor uniforme?

În celea ce urmează vor fi analizate două structuri matriceale cu dezvoltări de puteri care pot fi acceptate, în prima instanţă, candidate la reprezentarea unor matroide uniforme.

4. COOPTAREA MATRICELOR CLASICE

În teoria matricelor sunt cunoscute structuri matriceale pentru care *apriori* este ştiut că au determinantul diferit de zero. Printre acestea evidenţiem *matricele Vandermonde* (vezi, de exemplu, [5, 7]).

Conform definiţiei, matricea Vandermonde este matricea cu structura:

$$\mathbf{A}_{n\times n} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{bmatrix}. \qquad (11)$$

Uşor se observă că în cazul $a_i = \alpha^i$, $\alpha \in \mathbf{GF}(2^m)$ şi $\alpha \neq 0$, matricea (11) reprezintă tabelul de înmulţire asupra **GF**(2^m).

Pentru reprezentarea matroidelor uniforme vom aplica matricea (11) în forma:

$$\mathbf{GF}_{k\times n} = \begin{bmatrix} \alpha^0 & \alpha^1 & \dots & \alpha^{n-1} \\ \alpha^0 & \alpha^2 & \dots & \alpha^{n-1} \\ \vdots & \vdots & & \vdots \\ \alpha^0 & \alpha^{k-1} & \dots & \alpha^{(k-1)(n-1)} \end{bmatrix}, \qquad (12)$$

unde $\alpha \in \mathbf{GF}(2^m)$ şi $\alpha \neq 0$.

În sprijinul acestei propuneri vin următoarele considerente. În [4] a fost arătat că la decodarea unui cuvânt de cod recepţionat cu t erori este necesar de obţinut C_{n-t}^{k} rezultate (soluţii ale sistemelor de ecuaţii liniare) identice (acordate). Conform teoremei chineze despre resturi [8] codurile acordate la decodare pot fi reprezentate în forma ciclică. În acest caz, cuvintele de cod pot fi generate prin înmulţirea vectorului informaţional de lungimea k la matricea (12).

Aici trebuie de menţionat că (12) este cunoscută în teoria codurilor corectoare de erori ca matricea generatoare a codului ciclic Reed-Solomon [7, 8]. Să exemplificăm.

Exemplul 5. Fie **GF**(2^3) cu elementele prezentate în tabelul 6.

Tabelul 6. Reprezentarea elementelor câmpului **GF**(2^3) cu $p(x)= 1+x+x^3$.

Nr. crt.	Gradul α^j	Vector $x^2x^1x^0$	Valoare zecimală
0	$\alpha^{-\infty}$	000	0
1	α^0	001	1
2	α^1	010	2
3	α^2	100	4
4	α^3	011	3
5	α^4	110	6
6	α^5	111	7
7	α^6	101	5
8	$\alpha^7 \equiv \alpha^0$	001	1

Pentru (n, k)= (7, 3) avem:

$$G_{3\times 7} = \begin{bmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \alpha^0 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^1 & \alpha^3 & \alpha^5 \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{bmatrix}$$

sau

$$G_{3\times 7} = \begin{bmatrix} 1 & 2 & 4 & 3 & 6 & 7 & 5 \\ 1 & 4 & 6 & 5 & 2 & 3 & 7 \\ 1 & 3 & 5 & 4 & 7 & 2 & 6 \end{bmatrix}. \qquad (13)$$

Poate fi uşor verificat că determinantul oricărei submatrici de rangul 3 a matricei (13) este semnificativ. De aici rezultă că matricea (13) poate

$$G_{8\times16}=\begin{bmatrix}
1 & 2 & 4 & 8 & 16 & 32 & 64 & 128 & 195 & 69 & 138 & 215 & 109 & 218 & 119 & 238\\
1 & 4 & 16 & 64 & 195 & 138 & 109 & 119 & 31 & 124 & 51 & 204 & 182 & 157 & 49 & 196\\
1 & 8 & 64 & 69 & 109 & 238 & 124 & 102 & 182 & 249 & 196 & 239 & 116 & 38 & 243 & 148\\
1 & 16 & 195 & 109 & 31 & 51 & 182 & 49 & 150 & 116 & 76 & 74 & 42 & 229 & 72 & 10\\
1 & 32 & 138 & 238 & 51 & 175 & 196 & 58 & 76 & 148 & 168 & 36 & 10 & 131 & 13 & 99\\
1 & 64 & 109 & 124 & 182 & 196 & 116 & 243 & 42 & 18 & 10 & 197 & 52 & 158 & 86 & 164\\
1 & 128 & 119 & 102 & 49 & 58 & 243 & 84 & 72 & 80 & 13 & 79 & 86 & 139 & 190 & 193\\
1 & 195 & 31 & 182 & 150 & 76 & 42 & 72 & 160 & 52 & 61 & 41 & 206 & 129 & 45 & 68
\end{bmatrix}$$

Figura 2. Matricea matroidului uniform $U_{8,16}$.

fi acceptată în calitate de reprezentare a matroidului uniform $U_{3,7}$ asupra **GF**(2^3).

Să întărim acest succes. În figura 2 este prezentată matricea matroidului $U_{8,16}$ asupra **GF**(2^8) cu $p(x)= 1+ x+ x^6 + x^7 + x^8$. Prin verificare se constată că matricea $\mathbf{G}_{8\times16}$ într-adevăr reprezintă un matroid uniform.

Suntem "impuşi" să efectuăm verificarea (testarea) matricei $\mathbf{G}_{k\times n}$ deoarece din proprietatea că determinantul matricei Vandermonde este semnificativ (diferit de zero) încă nu rezultă că vor fi semnificative şi determinantele celorlalte submatrici ale matricei $\mathbf{G}_{k\times n}$. Complexitatea verificării matricei $\mathbf{G}_{k\times n}$ este dată de mărimea:

$$O(n,k)=C_n^k\cdot O(k),$$

unde $O(k)$ este complexitatea calculului determinantului matricei de dimensiunea $k\times k$, care se estimează prin:

$$O(k)=\sum_{i=3}^{k} i\big(O(i-1)+1\big),\ \text{unde } O(2)=3.$$

Încercarea de a extinde matricea (13) până la dimensiunea, de exemplu, $n= 9$ – un cod cu parametrii $(n, k, t)= (9, 3, 3)$, este sortită eşecului: matricea $G_{3\times9}$ va conţine două coloane, prima şi a noua, care se repetă de două ori. Acest eşec se explică prin faptul că un cod Reed-Solomon (RS) există numai pentru $n\le 2^m$-1. Iar pentru un cod matroid limita de sus a lui n este mai mare şi-i delimitată de următoarele propoziţii.

Propoziţia 2. Un matroid uniform $U_{k,n}$ de rangul $k= 2$ poate fi reprezentat asupra unui câmp **GF**(2^m) atunci şi numai atunci, dacă

$$n\le 2^m+ 1.$$

Propoziţia 3. Un matroid uniform $U_{k,n}$ de rangul $k= 3$ este reprezentabil asupra unui câmp $GF(2^m)$ numai pentru

$$n\le 2^m+ 2.$$

Propoziţia 4. Pentru $k\ge 2^m$ există numai $U_{k,k+1}$ asupra **GF**(2^m), $m= 2, 3, \ldots$

Este evident că în cazul $k= 1$ are loc inegalitatea:

$$n\le 2^m.$$

Prin transformări elementare matricea (12) poate fi adusă la, aşa numita, formă *canonică* sau *sistematică* :

$$\mathbf{G}_{k\times n}=[\mathbf{I}\ \mathbf{Q}], \qquad (14)$$

unde **I** este matricea-unitate:

$$\mathbf{I}_{k\times k}=\begin{bmatrix}
1 & 0 & \ldots & 0\\
0 & 1 & \ldots & 0\\
\vdots & \vdots & \ddots & \vdots\\
0 & 0 & \ldots & 1
\end{bmatrix}.$$

Matricea **I** întotdeauna defineşte o bază într-un spaţiu vectorial, inclusiv, şi asupra unui câmp finit.

Submatricea **Q** este de dimensiunea $k\times(n-k)$ şi putem impune acestei matrice, de exemplu, structura (12); avem:

$$\mathbf{Q}=\begin{bmatrix}
1 & \alpha^1 & \ldots & \alpha^{n-k-1}\\
1 & \alpha^2 & \ldots & \alpha^{2(n-k-1)}\\
\vdots & \vdots & & \vdots\\
1 & \alpha^{k-1} & \ldots & \alpha^{(k-1)(n-k-1)}
\end{bmatrix}. \qquad (15)$$

Exemplul 6. Fie **GF**(2^3), $p(x)=1+x+x^3$ şi codul $(n, k, t)= (10, 3, 3)$. Matricea sistematică de forma (14) este:

$$\mathbf{G}_{3\times10}=\big[\mathbf{I}_{3\times3}\ \mathbf{Q}_{3\times7}\big]=\begin{bmatrix}
1 & 0 & 0 & 1 & 2 & 4 & 3 & 6 & 7 & 5\\
0 & 1 & 0 & 1 & 4 & 6 & 5 & 2 & 3 & 7\\
0 & 0 & 1 & 1 & 3 & 5 & 4 & 7 & 2 & 6
\end{bmatrix}$$

Prin verificare se determină că matricea $\mathbf{G}_{3\times10}$ reprezintă un matroid uniform $U_{3,10}$ asupra **GF**(2^3).

Deci, acceptând *de facto* că o matrice de forma (14) poate reprezenta un matroid uniform, apare tentaţia de a genera matroidul unui cod corector de largă folosinţă. Cel mai uzual cod, la momentul actual, este RS-codul (n, k, t)= (28, 24, 2), aplicat în CD-ROMuri.

Pentru prezentarea matroidului $U_{24,28}$ de forma (14) este suficient de prezentat submatricea $\mathbf{Q}_{24\times4}$. Generăm această submatrice asupra câmpului $\mathbf{GF}(2^8)$ cu $p(x)= 1+ x+ x^6 + x^7 + x^8$; în figura 3 este prezentat rezultatul obţinut. Prin testarea determinantelor matricei $G_{24\times28}$ se stabileşte că ea reprezintă matroidul uniform $U_{24,28}$.

Revenind la problema căutării matroidelor, consemnăm că, în cazul reprezentării matroidului uniform $U_{k,n}$ printr-o matrice sistematică de forma (14), complexitatea algoritmului de căutare se va reduce la mărimea:

$$O(n,k) = (C_n^k - k - 1)\cdot O(k). \qquad (16)$$

Astfel, cooptarea matricei Vandermonde în calitate de bază constructivă pentru generarea matroidelor uniforme asupra câmpurilor Galois, a permis reducerea complexităţii algoritmului de căutare până la 1 (dacă nu se iau în consideraţie operaţiile (16) de verificare-testare a matricei **G**)! Cu toate acestea, la moment, se poate *numai* afirma că matricea de forma (14) *poate să reprezinte un matroid uniform*.

$$\mathbf{Q}_{24\times4}^{T} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 8 & 32 & 128 & 69 & 215 & 218 & 238 & 62 & 248 & 102 & 91 & 175 & 249 & 98 & 75 & 239 & 58 & 232 & 38 & 152 & 37 & 148 & 21 \\
4 & 64 & 138 & 119 & 124 & 204 & 157 & 196 & 29 & 19 & 243 & 235 & 168 & 18 & 227 & 40 & 197 & 13 & 208 & 158 & 244 & 155 & 164 & 210 \\
8 & 69 & 238 & 102 & 249 & 239 & 38 & 148 & 147 & 144 & 80 & 231 & 99 & 122 & 245 & 105 & 191 & 193 & 247 & 233 & 101 & 57 & 88 & 162
\end{bmatrix}$$

Figura 3. Matricea $\mathbf{Q}_{4\times24}$ generată asupra $\mathbf{GF}(2^8)$ cu $p(x)= 1+ x+ x^6 + x^7 + x^8$.

CONCLUZII

În acest articol nu s-a pus scopul de a rezolva în general, la nivel abstract, problema căutării matroidelor uniforme. Mai degrabă, este o încercare de a sonda subiectul matematic cu scopul de a găsi (cât mai repede) o soluţie *ad hoc*, dar *constructivă*, de generare a matroidelor cu *însemnătate* practică.

În articol a fost analizată problema căutării matroidelor uniforme $U_{k,n}$ asupra câmpurilor Galois extinse $\mathbf{GF}(2^m)$. Această problemă este strîns legată cu problema reprezentabilităţii matroidelor. În lucrare au fost găsite limitele de existenţă a matroidelor uniforme asupra $\mathbf{GF}(2^m)$. În particular, a fost stabilit că pentru $k\geq 2^m$ există numai $U_{k,k+1}$ asupra $\mathbf{GF}(2^m)$. Aceasta a permis restrângerea spaţiului de căutare, iar introducerea spre analiză a ciclocaselor a furnizat baza constructivă pentru generarea matricelor, candidate la reprezentarea matroidelor uniforme.

Analiza dezvoltărilor de puteri a adus la o soluţie particulară de reprezentare a matricelor matroidelor, şi anume, la forme sistematice, care includ în calitate de submatrice matricea Vandermonde, cunoscută în teoria codurilor corectoare de erori ca matricea generatoare a codului Reed-Solomon. Introducerea formei sistematice cu submatricea Vandermonde (Reed-Solomon) a permis generarea matroidelor uniforme de rang înalt, $k< 2^8$ (iar practic, nelimitat!).

În lucrare este prezentată matricea matroidului uniform $U_{24,28}$ care poate fi aplicată la construirea codecului CD-ROM. Nu-s contraindicaţii pentru generarea matroidelor uniforme cu parametrii acceptabili pentru codurile corectoare conforme, de exemplu, cu standardele MPEG.

Bibliografie

***1. Whitney H. On the abstract properties of linear dependence** // Amer. J. Math., Nr. 57, pag. 509..533, 1935.*

***2. Oxley J.G.** Matroid theory. Oxford University Press, New York, 1992.*

***3. Aigner M.** Combinatorial theory. Springer, New York, 1979.*

***4. Bodean G.** Aspecte teoretice ale codurilor matroide // Meridian ingineresc, Nr. 2, pag. 35..42, 2005.*

***5. Гантмахер Ф.Р.** Теория матриц. М.:Наука, 1988.*

***6. Lidl R., and Niederreiter H.** Finite fields. - Cambridge, University Press, 1997.*

***7. Blahut R.E.** Theory and Practice of Error-Control codes. Addison-Wasley Publ., Massachusetts, 1984.*

***8. Peterson W.W., and Weldon E.J.** Error-Correcting Codes. The MIT Press Cambridje, 1988.*

Aprobat spre publicare: 21.10.2005