Mariusz Frydrych[1,2], Maciej Kacperski[1,3], Grzegorz Zwoliński[1,3]
[1] Wyższa Szkoła Informatyki i Umiejętności
[2] Uniwersytet Łódzki, Wydział Matematyki i Informatyki
[3] Politechnika Łódzka, Instytut Mechatroniki i Systemów Informatycznych
e-mail: frydrych@wsinf.edu.pl, maciekka@wsinf.edu.pl, zwolinsk@wsinf.edu.pl

PEWNE RODZINY CHARAKTERYSTYCZNE KODÓW LINIOWYCH

Streszczenie – W pracy przedstawiono metodę generowania pewnych rodzin kodów liniowych nad ciałami skończonymi charakterystyki większej niż dwa w najobszerniejszej klasie ze względu na rozmiar rozmaitości Grassmanna, tzn. gdy wymiar jest równy kowymiarowi. Metoda oparta jest na zanurzeniu pewnej prostej rzutowej w rozmaitość Grassmana.

Słowa kluczowe: kodowanie, ciała skończone, kody liniowe, metryka Hamminga.

1 Wprowadzenie

Kody liniowe stosowane są powszechnie w przesyłaniu danych w zaszumianym medium transmisyjnym. Wymiar kodu to przepustowość łącza transmitowanej informacji. Z kolei kowymiar kodu, mierzy tak zwaną nadmiarowość, wielkość niezbędną do wykrywania i ewentualnej korekcji błędów przesyłanych danych. Liniowość kodu znakomicie upraszcza procesy kodowania i dekodowania, co skutkuje dużą wydajnością implementowanych algorytmów. Z oczywistych powodów, najczęściej stosuje się kody zero-jedynkowe, co znacznie zawęża spektrum możliwej do uzyskania jakości kodu. Zastosowanie większej liczby stanów (ciał skończonych charakterystyki większej niż dwa), daje elastyczną strukturę kolekcji kodów liniowych.

2 Ciała Galois

Folklor. Fq - ciało skończone (Galois) charakterystyki p = _(Fq), p - liczba pierwsza, q = pw, w ∈ N ([5], [1]).
Realizacja: f ∈ Fp[X], deg f = w - nieprzywiedlny wielomian stopnia w nad ciałem Fp = {0, 1, ….., p – 1}, Fq ≅ Fp[X]/(f).

Ciało Fq jest ciałem cyklotomicznym (grupa multiplikatywna $F^*q = Fq \setminus \{0\}$ jest grupą cykliczną), tzn. złożone jest z 0 i q -1 pierwiastków z jedynki stopnia $q-1 = p^w-1$. Istnieje $\xi \in$ Fq - pierwiastek pierwotny (jest ich $\varphi(q-1)$)

$$Fq = \{1, \xi, \xi^2, \xi^3, \xi^{q-2}\} \cup \{0\}. \tag{1}$$

Przykład. F16 - ciało 16-elementowe

$$\begin{aligned} &p = 2, \quad w = 4, \quad q = p^w = 16 \\ &f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X] \\ &f = (X - \xi^3) \cdot (X - \xi^6) \cdot (X - \xi^9) \cdot (X - \xi^{12}), \\ &\mathbb{F}_{16} = \{0, 1, \ldots, 9, a, \ldots, f\} \end{aligned}$$

$$\begin{aligned} \xi &= X^3 + X^2 + X &&= e \\ \xi^2 &= X^3 + 1 &&= 9 \\ \xi^3 &= X &&= 2 \\ \xi^4 &= X + 1 &&= 3 \end{aligned} \tag{2}$$

Przykład (c.d.)**.**

$$\begin{aligned} \xi^5 &= X^3 + X^2 + 1 &&= d \\ \xi^6 &= X^2 &&= 4 \\ \xi^7 &= X^2 + X &&= 6 \\ \xi^8 &= X^2 + 1 &&= 5 \\ \xi^9 &= X^3 &&= 8 \\ \xi^{10} &= X^3 + X^2 &&= c \\ \xi^{11} &= X^3 + X &&= a \\ \xi^{12} &= X^3 + X^2 + X + 1 &&= f \\ \xi^{13} &= X^2 + X + 1 &&= 7 \\ \xi^{14} &= X^3 + X + 1 &&= b \\ \xi^{15} &= 1 = \xi^0 &&= 1. \end{aligned} \tag{3}$$

Przykład (c.d.)**.**

$$\begin{aligned} a+c &= 6 \\ a\cdot c &= 4 \\ 2+3 &= 1 \\ 2\cdot 3 &= 6 \\ e+f &= 1 \\ e\cdot f &= 7 \\ a^{-1} &= 3 \\ c^{-1} &= d \\ e^{-1} &= b \\ f^{-1} &= 2 \end{aligned} \tag{4}$$

3 Kod liniowy

Niech, k, n, p, w, q ∈ N; p - liczba pierwsza; $q = p^w$, k ≤ n.

Definicja. Każdą k-wymiarową podprzestrzeń wektorową C przestrzeni n-wymiarowej F^n_q nazywamy kodem liniowym o długości n, wymiaru k, nad ciałem Fq ([4], [3]).

Uwaga. Wybór bazy B = (b_1, ..., b_k), b_1,....., b_k ∈ C ⊂ Fnq indukuje monomorfizm przestrzeni liniowych

$$\iota\colon \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n, \quad \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_k \end{pmatrix} \mapsto \sum_{j=1}^{k} \xi_j b_j, \quad \mathrm{im}(\iota) = C. \tag{5}$$

zwany kodowaniem liniowym.

Uwaga. Dostajemy

$$0 \longrightarrow \mathbb{F}_q^k \xrightarrow{\iota} \mathbb{F}_q^n \xrightarrow{\pi} \mathbb{F}_q^n/C \longrightarrow 0 \tag{6}$$

tzw. krótki ciąg dokładny przestrzeni wektorowych. codimC =dim Fnq/C = n-k. Składając π z dowolnym izomorfizmem $\mathrm{Fnq/C} \to F^{n-k}_q$ dostajemy ponownie (krótki ciąg dokładny). Operator (macierz) H nazywamy anihilatorem, macierzą kontrolną (check matrix) kodu C.

$$0 \longrightarrow \mathbb{F}_q^k \xrightarrow{\iota} \mathbb{F}_q^n \xrightarrow{H} \mathbb{F}_q^{n-k} \longrightarrow 0 \tag{7}$$

Uwaga. Kowymiar podprzestrzeni $\mathrm{codim}C = n - k$ to „ilość stopni kontrolnych kodu - nadmiarowość" a wymiar $\dim C = k$ „zawartość informacji".
Wektory bazowe $b_{1,\ldots,} b_k \in F_{nq}$ są liniowo niezależne, więc znajdziemy podciąg $1 <= j_1 < \ldots. < j_k <= n$, taki że macierz

$$b_{j_1,\ldots,j_k} = \begin{bmatrix} b_{j_1,1} & \ldots & b_{j_1,k} \\ \vdots & \vdots & \vdots \\ b_{j_k,1} & \ldots & b_{j_k,k} \end{bmatrix} \tag{8}$$

jest nieosobliwa.
Uwaga (c.d.)**.**

$$P \cdot B \cdot b^{-1}_{j_1,\ldots,k_k} = \begin{bmatrix} 1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 1 \\ a_{1,1} & \ldots & a_{1,k} \\ \vdots & \ddots & \vdots \\ a_{n-k,1} & \ldots & a_{n-k,k} \end{bmatrix} \tag{9}$$

P jest odpowiednią macierzą permutacji osi współrzędnych przestrzeni F_{nq}. Jest to tzw. standardowa postać bazowa kodu liniowego C.

Uwaga. Dla postaci standardowej kodu C

$$B = \begin{bmatrix} I_{k,k} \\ A \end{bmatrix} \tag{10}$$

anihilator (macierz kontrolna, check matrix) H ma postać

$$H = \begin{bmatrix} -A & I_{n-k,n-k} \end{bmatrix} \tag{11}$$

gdzie $I_{k,k}$, $I_{n-k,n-k}$ są macierzami jednostkowymi odpowiednich wymiarów.

4 Metryka Hamminga

Definicja. Rozszerzają˛c metryke˛ dyskretna˛ (jedyna˛) w ciele Fq

$$\|x\| = \begin{cases} 0 & dla \quad x = 0 \\ 1 & dla \quad x \neq 0 \end{cases} \tag{12}$$

do normy L^1 w przestrzeni wektorowej Fnq wzorem

$$\|v\| = \sum_{j=1}^{n} \|v_j\|, \; v = (v_1, \ldots, v_n). \tag{13}$$

otrzymujemy, tzw. metrykę Hamminga

$$\varrho \colon \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{Z}_+, \;\; \varrho(u, v) = \|u - v\|. \tag{14}$$

Definicja. Dla kodu liniowego $C \subset F^n_q$ liczbę

$$d = \min_{u,v \in C, u \neq v} \varrho(u, v) = \min_{u,v \in C, u \neq v} \|u - v\| = \min_{v \in C, v \neq 0} \|v\|. \tag{15}$$

nazywamy minimalną odległością Hamminga lub krócej odległością Hamminga ([2]).

Stwierdzenie. Odległość Hamminga kodu $C \subset F^n_q$ jest równa minimalnej liczbie liniowo zależnych kolumn anihilatora kodu C.

Możemy wykryć d błędów kodu C oraz skorygować $\lfloor \frac{d-1}{2} \rfloor$ błędów ([2]).

5 Grassmanian

Definicja. Ogół wszystkich podprzestrzeni k-wymiarowych przestrzeni n-wymiarowej F^n_q nazywamy rozmaitością Grassmana lub Grassmanianem i oznaczamy

$$Grass(k, n, \mathbb{F}_q) = \{V : V \subset \mathbb{F}_q^n \wedge \dim_{\mathbb{F}_q} V = k\}. \tag{16}$$

Uwaga. Z postaci standardowej widać, że Grassmanian $Grass(k, n, F_q)$ jest rozmaitością wymiaru $k\ (n - k)$ nad ciałem Fq i można go naturalnie zanurzyć jako kwadrykę w przestrzeni rzutowej

$$Grass(k, n, \mathbb{F}_q) \hookrightarrow \mathbb{P}(\Lambda^k \mathbb{F}_q^n)$$

$$\operatorname{span}(v_1, \ldots, v_k) \mapsto \operatorname{span}(v_1 \wedge \ldots \wedge v_k). \tag{17}$$

Pełna grupa liniowa $GL(F^n_q)$ działa tranzytywnie na podprzestrzeniach ustalonego wymiaru, stąd

Stwierdzenie. Grassmanian jest przestrzenią jednorodna

$$Grass(k,n,\mathbb{F}_q) \simeq GL(\mathbb{F}_q^n)/F(k,n,\mathbb{F}_q) \tag{18}$$

F(k, n, Fq) jest grupą macierzy postaci

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \tag{19}$$

gdzie

$$a \in GL(\mathbb{F}_q^k), \quad c \in GL(\mathbb{F}_q^{n-k}), \quad b \in M(k, n-k, \mathbb{F}_q). \tag{20}$$

b jest dowolną macierzą prostokątną o k wierszach i n-k kolumnach i elementach w ciele Fq.

Ponieważ grupa liniowa składa się z

$$\begin{aligned} \#\ GL(\mathbb{F}_q^n) &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) \\ &= (q^n-1)(q^{n-1}-1)\cdots(q-1)\cdot q^{\binom{n}{2}} \end{aligned} \tag{21}$$

elementów, otrzymujemy

Wniosek. Liczba elementów rozmaitości Grassmana wynosi

$$\#\ Grass(k,n,\mathbb{F}_q) = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}. \tag{22}$$

Przykład. Zestawienie: k - wymiar kodu, n - długość kodu, q - ilość elementów w ciele Fq, # [k, n]q - ilość elementów Grassmanianu Grass(k, n, Fq).

$$\begin{bmatrix} k & n & q & \#\,[k,n]_q \\ 2 & 4 & 2 & 35 \\ 2 & 4 & 2^4 & 70\,161 \\ 4 & 7 & 2 & 11\,811 \\ 4 & 7 & 2^2 & 24\,208\,613 \\ 4 & 7 & 2^3 & 79\,936\,505\,481 \\ 4 & 7 & 2^4 & 301\,490\,686\,407\,185 \\ 2 & 7 & 2 & 2\,667 \\ 2 & 7 & 2^4 & 1\,177\,411\,592\,721 \\ 4 & 8 & 2 & 200\,787 \\ 4 & 8 & 2^4 & 19\,758\,795\,115\,067\,683\,345 \\ 8 & 16 & 2 & 63\,379\,954\,960\,524\,853\,651 \\ 2 & 4 & 7 & 2\,850 \\ 2 & 4 & 7^2 & 5\,887\,302 \\ 3 & 6 & 7 & 48\,177\,200 \\ 3 & 6 & 7^2 & 1\,663\,045\,363\,565\,300 \end{bmatrix} \tag{23}$$

6 Generowanie szczególnych kodów

Konstrukcja. Rozważmy teraz liczbę pierwszą $p > 2$, oraz liczby naturalne k, $n = 2k$. Będziemy poszukiwać k-wymiarowych kodów liniowych o długości n, tzn. długość kodu będzie równa podwojonemu wymiarowi.
Grassmanian $\mathrm{Grass}(k, 2k, F_p)$ jest „najbogatszy w wymiarze połówkowym” bowiem składa się z

$$\frac{(p^{2k}-1)(p^{2k-1}-1)\cdots(p^{k+1}-1)}{(p^k-1)(p^{k-1}-1)\cdots(p-1)} \tag{24}$$

elementów.
Przestrzeń wektorową F^n_p nad ciałem F_p możemy potraktować jako ciało F_{p^n} poprzez rozszerzenie stopnia n ciała prostego F_p za pomocą nieprzywiedlnego wielomianu $f \in F_p[X]$; $\deg f = n$.
Od tej pory będziemy w powyższy sposób utożsamiać ciało F_{p^n} z przestrzenią liniową F^n_p nad ciałem F_p:

$$\mathbb{F}_{p^n} \simeq_f \mathbb{F}_p^n. \tag{25}$$

Rozważmy automorfizm Frobeniusa

$$\sigma : \mathbb{F}_p^n \to \mathbb{F}_p^n, \quad \sigma(x) = x^p, \tag{26}$$

którego n-ta iteracja

$$\sigma^n(x) = x^{p^n} \tag{27}$$

jest identycznością (Id = 1) na F_p^n. Ponieważ n = 2k, to k-ta iteracja $\sigma^k(x) = x^{p^k}$ jest inwolucją. Oznaczmy ją przez τ.
Otrzymaliśmy operator liniowy

$$\tau : \mathbb{F}_p^n \to \mathbb{F}_p^n, \quad \tau^2 = 1, \tag{28}$$

który w naturalny sposób rozkłada przestrzeń F_p^n na sumę prostą dwóch podprzestrzeni własnych:

$$V^+ = \ker(\tau - 1), \quad V^- = \ker(\tau + 1)$$
$$\mathbb{F}_p^n = V^+ \oplus V^- \tag{29}$$

Ponieważ charakterystyka ciała jest różna od dwóch, dostajemy dwa operatory idempotentne (rzuty)

$$\pi^+, \pi^- : \mathbb{F}_p^n \to \mathbb{F}_p^n$$
$$\pi^+ = \frac{1}{2}(1 - \tau), \quad \pi^- = \frac{1}{2}(1 + \tau), \tag{30}$$

spełniające warunki:

$$\pi^+ + \pi^- = 1,$$
$$\pi^+\pi^- = 0 = \pi^-\pi^+,$$
$$\ker \pi^+ = \operatorname{im} \pi^- = V^+,$$
$$\ker \pi^- = \operatorname{im} \pi^+ = V^-. \tag{31}$$

Z drugiej strony zauważmy, że

$$V^+ = \ker \pi^+ = \ker(1-\tau) = \ker(1-\sigma^k), \tag{32}$$

co oznacza, że V^+ jest rozszerzeniem stopnia k ciała prostego F_p, tzn. jest izomorficzne z ciałem skończonym p^k-elementowym F_{p^k}.
Podsumowując, otrzymaliśmy ciąg kolejnych ciał, rozszerzeń ciała prostego F_p:

$$\mathbb{F}_p \subsetneq V^+ \subsetneq \mathbb{F}_p^n \tag{33}$$

gdzie

$$V^+ \simeq \mathbb{F}_{p^k}, \quad \mathbb{F}_p^n \simeq \mathbb{F}_{p^n}. \tag{34}$$

$$|V^+ : \mathbb{F}_p| = k, \ |\mathbb{F}_p^n : V^+| = 2, \ |\mathbb{F}_p^n : \mathbb{F}_p| = n = 2k. \tag{35}$$

Kluczowe dla naszej konstrukcji jest rozszerzenie stopnia dwa F_{np}/V^+ ciała p^k-elementowego V^+ przez ciało p^n-elementowe F_{p^n}. Mianowicie, traktujemy ciało F_{p^n} jako dwuwymiarową przestrzeń wektorową nad ciałem V^+. Automofizm ciała F_{p^n} jako operator liniowy nad ciałem prostym F_p

$$\tau : \mathbb{F}_p^n \to \mathbb{F}_p^n \tag{36}$$

jest niezmienniczy na podprzestrzeni V^+, więc możemy go traktować jako operator liniowy nad ciałem $V^+ \cong F_{p^k}$.
Jeżeli wybierzemy dowolny element $\xi \in V^-$, $\xi \neq 0$ to mnożenie przez ξ^{-1} ustala izomorfizm pomiędzy podprzestrzeniami:

$$\xi^{-1} : V^- \to V^+, \quad \xi^{-1}(x) = \xi^{-1} \cdot x \tag{37}$$

a izomorfizmem odwrotnym jest:

$$\xi : V^+ \to V^-, \quad \xi(x) = \xi \cdot x \tag{38}$$

Ponieważ $\xi^2 \in V^+, \xi \notin V^+$ to $\mathbb{F}_p^n \simeq V^+[\xi]$, tzn. element ξ realizuje rozszerzenie F^n_p/V^+ stopnia dwa.
W powyższy sposób dostajemy rozkład ciała F^n_p na sumę prostą podprzestrzeni liniowych

$$\begin{aligned} \mathbb{F}_p^n &\simeq_\xi V^+ \oplus V^+ \\ \mathbb{F}_p^n \ni u &\mapsto (\xi^{-1} \cdot \pi^+ u, \pi^- u) \in V^+ \oplus V^+ \end{aligned} \tag{39}$$

Każdej jednowymiarowej (nad $V^+ \cong F_{p^k}$) podprzestrzeni wektorowej odpowiada naturalnie k-wymiarowa (nad F_p) podprzestrzeń liniowa przestrzeni F^n_p.

$$\Theta : \mathbb{P}^1(\mathbb{F}_{p^k}) \longrightarrow Grass(k, 2k, \mathbb{F}_p). \tag{40}$$

Wykorzystując współrzędne jednorodne, prostą rzutową $P^1(F_{p^k})$ możemy utożsamić z $\mathbb{F}_{p^k} \cup \{\infty\}$

$$(V^+ \oplus V^+)/\mathbb{F}_{p^k} \ni [x, y] \longmapsto \begin{cases} \dfrac{x}{y} & dla \quad y \neq 0 \\ \infty & dla \quad y = 0. \end{cases} \tag{41}$$

Jawna postać włożenia Θ wygląda następująco:

$$\mathbb{F}_{p^k} \simeq V^+ \ni x \longmapsto \mathrm{span}_{\mathbb{F}_{p^k}}\{x + \xi\} \subset \mathbb{F}_p^n$$

$$\infty \longmapsto V^+ \subset \mathbb{F}_p^n. \tag{42}$$

Przykład. Aby zilustrować powyższą konstrukcję rodzin kodów liniowych rozważmy ciało skończone F_{7^6} rzędu $7^6 = 117\,649$ przyjmując następujące wartości parametrów:

$$p = 7,\ k = 3,\ n = 2k = 6, \tag{43}$$

wielomian nieprzywiedlny $f \in F_7[X]$ stopnia $n = 6$:

$$f(X) = X^6 + X^5 + 2X^4 + X^3 + 5X^2 + 3X + 2, \tag{44}$$

generator (pierwiastek pierwotny) g ciała F_{7^6} rzędu $7^6 - 1 = 117\,648$

$$g(X) = 3X^5 + 4X^4 + 5X^2 + 2X + 2. \tag{45}$$

Realizacją ciała F_{7^6} jest ucięta algebra wielomianów:

$$\mathbb{F}_{7^6} \simeq \mathbb{F}_7[X]/(f). \tag{46}$$

Obliczenia będziemy prowadzić w uporządkowanej bazie sześciowymiarowej przestrzeni wektorowej $F_{7^6} \cong F_{67}$ nad ciałem F_7:

$$(X^5, X^4, X^3, X^2, X, 1). \tag{47}$$

Macierze automorfizmu Frobeniusa $\sigma : \mathbb{F}_7^6 \to \mathbb{F}_7^6$ oraz inwolucja $\tau = \sigma^3$:

$$\sigma = \begin{bmatrix} 6 & 0 & 2 & 5 & 6 & 0 \\ 4 & 5 & 6 & 4 & 1 & 0 \\ 2 & 3 & 5 & 1 & 3 & 0 \\ 4 & 2 & 1 & 3 & 2 & 0 \\ 2 & 4 & 3 & 6 & 1 & 0 \\ 6 & 6 & 4 & 6 & 2 & 1 \end{bmatrix}, \quad \tau = \begin{bmatrix} 3 & 5 & 5 & 0 & 5 & 0 \\ 6 & 5 & 0 & 3 & 5 & 0 \\ 4 & 4 & 6 & 2 & 1 & 0 \\ 1 & 2 & 5 & 1 & 6 & 0 \\ 1 & 2 & 5 & 2 & 5 & 0 \\ 6 & 2 & 3 & 6 & 2 & 1 \end{bmatrix} \tag{48}$$

operatory rzutu (idempotenty) π^+ *i* π^-:

$$\pi^+ = \begin{bmatrix} 6 & 1 & 1 & 0 & 1 & 0 \\ 4 & 5 & 0 & 2 & 1 & 0 \\ 5 & 5 & 1 & 6 & 3 & 0 \\ 3 & 6 & 1 & 0 & 4 & 0 \\ 3 & 6 & 1 & 6 & 5 & 0 \\ 4 & 6 & 2 & 4 & 6 & 0 \end{bmatrix}, \quad \pi^- = \begin{bmatrix} 2 & 6 & 6 & 0 & 6 & 0 \\ 3 & 3 & 0 & 5 & 6 & 0 \\ 2 & 2 & 0 & 1 & 4 & 0 \\ 4 & 1 & 6 & 1 & 3 & 0 \\ 4 & 1 & 6 & 1 & 3 & 0 \\ 3 & 1 & 5 & 3 & 1 & 1 \end{bmatrix} \tag{49}$$

bazy podprzestrzeni V^+ *i* V^- (jako odpowiednie kolumny macierzy):

$$V^+ = \begin{bmatrix} 6 & 1 & 0 \\ 5 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad V^- = \begin{bmatrix} 3 & 1 & 2 \\ 0 & 4 & 5 \\ 6 & 4 & 6 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{50}$$

elementy $\xi,\ \xi^{-1} \in V^-$:

$$\xi = 2X^5 + 6X^4 + 5X^3 + 5X^2 + 4, \quad \xi^{-1} = 3X^5 + 6X^3 + X^2. \tag{51}$$

Dla ujednolicenia oznaczeń, bazą przestrzeni $\mathrm{F}^6{}_7$ jest

$$(X^5, X^4, X^3, X^2, X, 1) = (e_1, e_2, e_3, e_4, e_5, e_6) \tag{52}$$

oraz baza podprzestrzeni V^+

$$\begin{aligned} f_1 &= 6e_1 + 5e_2 + e_3 \\ f_2 &= e_1 + e_4 + e_5 \\ f_3 &= e_6. \end{aligned} \tag{53}$$

Mnożenie w ciele F^6_7 można przedstawić jako tensor

$$\begin{gathered} \mathbb{F}_7^6 \otimes_{\mathbb{F}_7} \mathbb{F}_7^6 \longrightarrow \mathbb{F}_7^6 \\ e_j \cdot e_k = \sum_{l=1}^{6} c_{j,k}^l e_l, \quad j,k = 1,\ldots,6 \end{gathered} \tag{54}$$

gdzie współczynniki $c_{j,k}^l \in \mathbb{F}_7$ są stałymi struktury (mnożenia).
Gdy mnożenie przez lewy czynnik ograniczymy do podprzestrzeni $V^+ \simeq \mathbb{F}_{7^3}$ to otrzymamy częściowy tensor w postaci trzech macierzy

$$f_{1\cdot} = \begin{bmatrix} 0 & 6 & 6 & 4 & 6 & 6 \\ 2 & 6 & 5 & 3 & 3 & 5 \\ 3 & 0 & 4 & 6 & 1 & 1 \\ 0 & 2 & 6 & 1 & 5 & 0 \\ 5 & 2 & 4 & 5 & 3 & 0 \\ 2 & 2 & 6 & 2 & 2 & 0 \end{bmatrix}, \quad f_{2\cdot} = \begin{bmatrix} 1 & 3 & 3 & 6 & 6 & 1 \\ 4 & 4 & 6 & 2 & 5 & 0 \\ 1 & 3 & 3 & 4 & 0 & 0 \\ 6 & 4 & 6 & 2 & 3 & 1 \\ 6 & 0 & 5 & 1 & 4 & 1 \\ 1 & 1 & 2 & 2 & 5 & 0 \end{bmatrix}, \quad f_{3\cdot} = Id. \tag{55}$$

Włożenie generujące $7^3 + 1 = 344$ kodów liniowych

$$\Theta : \mathbb{P}^1(\mathbb{F}_{7^3}) \longrightarrow Grass(3, 6, \mathbb{F}_7) \tag{56}$$

realizujemy teraz następująco:

$$\begin{gathered} \mathbb{F}_{7^3} \simeq V^+ \ni x \longmapsto \mathrm{span}_{\mathbb{F}_{7^3}}\{x + \xi\} \subset \mathbb{F}_7^6 \\ \infty \longmapsto V^+ \subset \mathbb{F}_7^6. \end{gathered} \tag{57}$$

Ogólnie, każda podprzestrzeń jednowymiarowa nad F_{7^3} jest odwzorowywana na podprzestrzeń wymiaru trzy nad F_7 za pomocą operacji

$$\mathbb{F}_7^6 \ni u, \quad \mathrm{span}_{\mathbb{F}_{7^3}}\{u\} \mapsto \mathrm{span}_{\mathbb{F}_7}\{f_1 \cdot u, f_2 \cdot u, f_3 \cdot u\}. \tag{58}$$

7 Podsumowanie

Praca opisuje metodę szybkiego generowania kodów liniowych w wymiarze „połówkowym", tzn. gdy wymiar kodu jest równy jego kowymiarowi. Kod jest reprezentowany w przestrzeni wektorowej nad ciałem skończonym charakterystyki większej niż dwa, co dało możliwość wykorzystania automorfizmu Frobeniusa do konstrukcji pewnych operatorów liniowych mających naturę geometryczną. Metodę zilustrowano przykładem w wymiarze trzy (wymiar i kowymiar kodu) nad ciałem charakterystyki siedem.

8 Literatura

[1] Winter D., *The Structure of Fields*. Springer-Verlag New York-Heidelberg-Berlin, 1974.

[2] MacWilliams F.J., Sloane N.J.A., *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1978.

[3] Pless V., *Introduction to the Theory of Error-Correcting Codes*.. John Wiley and Sons, Inc., 1998.

[4] Biswas S., *Introduction to Codding Theory: Basic codes and Shannon's theorem*. Internet, 2011.

[5] Browkin j., *Teoria ciał*. PWN, Biblioteka Matematyczna, tom 49, 1978.

SOME CHARACTERISTIC FAMILIES OF LINEAR CODES

Summary: The paper presents a method to generate some families of linear codes over finite fields of characteristics greater than two in the widest class due to the size of Grassmann manifold, i.e. when the dimension is equal to codimension. Our method applies some simple embedding of projective line into the Grassman manifold.

Keywords: codding, finite fields, linear codes, Hamming metrics.