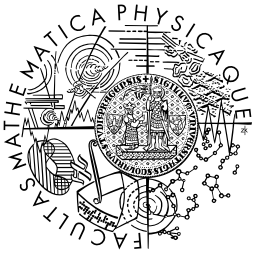

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Lukáš Belza

Konstrukce MDS matic

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Studijní program: Matematika
Studijní obor: Matematika pro informační technologie

Praha 2021

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V Praze dne 7. ledna 2021 .....

Podpis autora

Poděkování
Tímto bych chtěl poděkovat především vedoucímu mé bakalářské práce, docentu Janu Žemličkovi, za podnětné rady a trpělivost při jejím psaní. Děkuji také docentu Alexandru Kazdovi za odbornou konzultaci. V neposlední řadě patří můj dík také rodině a přítelkyni za podporu, kterou mi při psaní této práce věnovali.

Název práce: Konstrukce MDS matic

Autor: Lukáš Belza

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: Tato práce se zaměřuje na takzvané Maximum Distance Separable (zkráceně MDS) matice nad konečnými tělesy, především pak na cirkulantní MDS matice. Na začátku jsou představeny koncepty související s MDS kódy a jejich charakterizací. Poté následuje úvod do cirkulantních matic a jejich vztah k faktorovým algebrám polynomů. Druhá část se zaměřuje především na cirkulantní MDS matice. Vychází z konstrukce MDS matic tvaru 3×3 a 4×4 a poté pokračuje obecnou konstrukcí MDS matic z Vandermondových matic. Nakonec uvádí určitá omezení týkající se existence ortogonálních cirkulantních MDS matic, konkrétně že neexistují žádné takové matice tvaru $2^d \times 2^d$ nad žádným konečným tělesem charakteristiky dva.

Klíčová slova: MDS matice, Cirkulantní matice, Biregulární matice, Kryptografie

Title: Construction of MDS matrices

Author: Lukáš Belza

Department: The Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., The Department of Algebra

Abstract: This thesis focuses on Maximum Distance Separable (MDS) matrices over finite fields, with emphasis on circulant MDS matrices. At the beginning, concepts related to MDS codes and their characterization are introduced. This is directly followed by an introduction into circulant matrices and their relation to factor algebras of polynomials. In the second part, we shift our focus specifically on circulant MDS matrices. We start from the construction of such matrices in dimensions 3×3 and 4×4 and then proceed to a general construction of MDS matrices from Vandermond matrices. Finally, we find some restrictions on the existence of orthogonal circulant MDS matrices, namely that there are no such $2^d \times 2^d$ matrices over any finite field of characteristic two.

Keywords: MDS matrix, Circulant matrix, Bi-regular matrix, Cryptography

Obsah

Úvod

V roce 1998 francouzský kryptograf a profesor Serge Vaudenay představil takzvanou dekorelační teorii pro návrh blokových šifer dokazatelně bezpečných vůči diferenciální a lineární kryptoanalýze. Vaudenay navrhl používání takzvaných Maximum Distance Separable matic, zkráceně MDS. Tyto matice se vyznačují značnou difúzní vlastností, změna nepatrné části vstupu tak změní velkou část výstupu. MDS matice nacházejí uplatnění v difúzní vrstvě některých blokových šifer jako je AES nebo Twofish a také v hashovací funkci Whirlpool.

S MDS maticemi se můžeme setkat třeba také v teorii kódování, konkrétně u Reed-Solomonových kódů. Tyto kódy se vyznačují maximální možnou minimální (takzvanou Hammingovou) vzdáleností kódových slov při dané délce a dimenzi kódu. Našly využití v komunikačním standardu pro digitální mobilní sítě GSM, datových úložištích jako je CD, DVD nebo Blu-Ray či ve standardu digitálního televizního vysílání DVB.

Právě konstrukce těchto matic, především pak cirkulantních MDS matic nad konečným tělesem pro využití v kryptografii, je tématem mé bakalářské práce.

V první kapitole se budu zabývat MDS maticemi. Tyto matice charakterizuji pomocí regularity jejich podmatic. Dále se zaměřím na cirkulantní matice, které mohou posloužit jako dobrý základ pro konstrukci MDS matic v následující kapitole. Nakonec se budu zabývat vztahy mezi cirkulantními a MDS maticemi, konkrétně otázkou, za jakých podmínek může být matice cirkulantní a zároveň MDS.

Ve druhé kapitole se budu věnovat samotné konstrukci MDS matic. Použiji při tom nástroje z předchozí kapitoly a znalosti konečných těles. Krátce uvedu, že nalezením jedné cirkulantní MDS matice lze získat hned několik MDS cirkulantních matic. Vytvořím cirkulantní MDS matice tvaru 3×3 a za pomoci minimálního polynomu prvku $\alpha \in \mathbb{F}_{2^n}$ zkonstruuji cirkulantní MDS matice tvaru 4×4. Následně charakterizuji MDS cirkulantní matice tvaru 4×4 nad konečným i obecným tělesem. Pustím se také krátce do obecnějších konstrukcí MDS matic pomocí Vandermondových matic a kapitolu uzavřu tvrzením o neexistenci ortogonálních cirkulantních MDS matic tvaru $2^d \times 2^d$ nad tělesem charakteristiky dva.

V poslední kapitole krátce naznačím využití MDS matic v kryptografii. Konkrétně půjde o jednu z matic zkonstruovaných v předchozí kapitole, která má své místo v kryptografickém standardu AES.

1. Vlastnosti MDS, Cirkulantních a Biregulárních matic

V této kapitole se zaměříme na zadefinování a vlastnosti MDS, cirkulantních a biregulárních matic. Kapitola vychází především z článku [1].

1.1 MDS matice

Použijeme definice a tvrzení ze skript samoopravných kódů [2], [3] a ze skript lineární algebry [4].

Mějme těleso $\mathbb{F}$, lineární kód C je podprostor vektorového prostoru $\mathbb{F}^n$ určený trojicí parametrů $[n, k, d]$, kde n značí jeho délku, k jeho dimenzi a d minimální vzdálenost jednotlivých prvků kódu C, tj. kódových slov. Minimální vzdáleností rozumíme Hammingovu vzdálenost, tedy počet pozic, na kterých se kódová slova liší. Kód C dimenze k obsahuje $|C| = |\mathbb{F}|^k$ kódových slov. Někdy se pro kód C používá zkrácené značení $[n, k]$-kód.

Definice 1 (Standardní tvar matice)**.** *Řekneme, že matice A tvaru $k \times n$ je* ve standardním tvaru*, jestliže $A = [I_k|B]$, kde I_k značí jednotkovou matici tvaru $k \times k$ a B je libovolná matice tvaru $k \times (n - k)$.*

Definice 2 (Generující matice kódu)**.** *Matice G tvaru $k \times n$, jejíž řádky generují $[n, k]$-kód C, se nazývá* generující matice kódu C*.*

Definice 3 (Prověrková matice kódu)**.** *Pro $[n, k]$-kód C nazveme matici H tvaru $(n - k) \times n$* prověrkovou maticí kódu C *právě tehdy, když $u \in C \Leftrightarrow Hu^T = 0$.*

Tvrzení 1. [2, Tvrzení 1.1] *Ať $G = [I_k|A]$ je generující maticí kódu C ve standardním tvaru, potom $H = [-A^T|I_{n-k}]$ je prověrkovou maticí kódu C.*

Tvrzení 2. [2, Tvrzení 2.6] *Ať C je $[n, k, d]$-kód s prověrkovou maticí H. Potom je $d - 1$ rovno největšímu číslu r takovému, že každých r sloupců matice H je lineárně nezávislých.*

Důsledek 3 (Singletonův odhad)**.** [2, Důsledek 2.7] *Pro $[n, k, d]$-kód C platí nerovnost $n - k \geq d - 1$.*

Singletonův odhad dává do souvislosti délku, dimenzi a minimální vzdálenost kódu. Na jeho základě je možné definovat takzvané MDS kódy, které jsou v tomto ohledu extrémním případem.

Definice 4 (MDS kód)**.** *Lineární $[n, k, d]$-kódy, pro které platí $n - k = d - 1$, nazýváme* MDS kódy*.*

MDS kód je tedy lineární kód délky n, dimenze k a minimální vzdálenosti $d = n - k + 1$. Jedná se o kódy, které mají při dané délce a dimenzi maximální možnou minimální vzdálenost.

Lemma 4. [3, Důsledek 6.1.2] *Nechť C je $[n,k]$-kód s generující maticí G. Pak C je MDS právě tehdy, když je každá k-tice sloupců matice G lineárně nezávislá.*

Definice 5 (MDS matice)**.** *Nechť $\mathbb{F}$ je těleso a n, k jsou dvě přirozená čísla splňující $n > k > 0$. Řekneme, že matice M tvaru $k \times (n-k)$ je* MDS*, pokud je pro $G = [I_k|M]$ množina řádkových vektorů $\{xG \mid x \in \mathbb{F}^k\}$ MDS kód.*

Definice 6 (Čtvercová podmatice)**.** *Pro matici A tvaru $m \times n$ definujeme* čtvercovou podmatici *M tvaru $s \times s$, kde $1 \leq s \leq \min(m,n)$, jako matici tvořenou hodnotami matice A výběrem s řádků a s sloupců matice A.*

Příklad. Pro obecnou matici A tvaru $m \times n$, kde $m, n \geq 2$, máme podmatici M tvaru 2×2:

$$M = \begin{pmatrix} a_{i,i} & a_{i,j} \\ a_{j,i} & a_{j,j} \end{pmatrix} \qquad \text{pro libovolná } i,j \in \{1,\ldots,\min(m,\,n)\},\ i<j.$$

Někdy je užitečné matici **přeskládat**, tedy zpermutovat její řádky a sloupce tak, aby bylo možné s ní lépe pracovat. Přeskládání matice nemění její determinant až na znaménko. Permutací sloupců dojde pouze ke změně pořadí souřadnic obrazů, tedy kódových slov. Uvažujeme-li generující matici kódu C, parametry $[n,k,d]$ jsou vůči přeskládání invariantní.

Věta 5 (Charakterizace MDS kódu)**.** [1, Theorem 1] *Nechť C je $[n,k,d]$-kód s generující maticí $G = [I_k|A]$, kde A je matice tvaru $k \times (n-k)$. Potom je C MDS kód právě tehdy, když je každá čtvercová podmatice A regulární.*

Důkaz: $\Longleftarrow$
Každá čtvercová podmatice A je regulární. Z [4, Věta 5.88] víme, že

$$\dim(\mathrm{Im}(A)) = \dim(\mathrm{Im}(A^T)),$$

tedy každá čtvercová podmatice $-A^T$ je také regulární. Z Tvrzení 1 víme, že $H = [-A^T|I_{n-k}]$ tvaru $(n-k) \times n$ je prověrková matice kódu C. Zbývá dokázat, že má každých $n-k$ sloupců lineárně nezávislých, pak z Tvrzení 2 dostaneme rovnost $d-1 = n-k$.

Z matice H vytvoříme čtvercovou podmatici B tvaru $(n-k)\times(n-k)$ výběrem i sloupců z matice $-A^T$ a $n-k-i$ sloupců z matice I_{n-k}. Chceme dokázat, že matice B je regulární.

V případě, že $i = 0$, dostáváme $B = I_{n-k}$, což je zřejmě regulární matice.

Předpokládejme, že $i \geq 1$.

- Buď $k < n-k$, pak jsme pro libovolné $i \in \{1,\ldots,k\}$ vytvořili podmatici B matice H. Tuto podmatici přeskládáme tak, že jako prvních $n-k-i$ sloupců vezmeme sloupce matice I_{n-k} a přeskládáme řádky, tak aby prvních $n-k-i$ řádků a sloupců přeskládané matice B' tvořilo jednotkovou matici I_{n-k-i}. Zbylých i sloupců a řádků je podmaticí $-A^T$ a tvoří tak regulární matici M tvaru $i \times i$. Protože přeskládání matice mění pouze znaménko jejího determinantu, existuje $j \in \mathbb{N}$ takové, že

  $$(-1)^j \det(B) = \det(B') = \det(M) \neq 0,$$

  kde druhá rovnost plyne z Věty o rozvoji podle sloupce [4, Věta 7.32]. Matice B je tedy regulární.

- Buď naopak $k \geq n-k$, pak pro libovolné $i \in \{1, \ldots, n-k-1\}$ postupujeme analogicky jako v předchozím případě. Pro $i = n-k$ plyne regularita podmatice B z regularity každé podmatice matice $-A^T$.

Dokázali jsme, že matice B je regulární. Prověrková matice $[-A^T|I_{n-k}]$ tvaru $(n-k) \times n$ má proto každých $n-k$ sloupců lineárně nezávislých, podle Tvrzení 2 tedy $d-1 = n-k$ a kód je tak podle definice MDS.

$\Longrightarrow$

C je MDS kód, platí tedy $d-1 = n-k$. Z tvrzení (2) je potom každých $n-k$ sloupců prověrkové matice $H = [-A^T|I_{n-k}]$ lineárně nezávislých.

Označme $p = \min(n-k, k)$ velikost největší čtvercové podmatice matice A. Zvolme libovolné $i \in 1, \ldots, p$, k němu libovolnou podmnožinu X indexů řádků matice A tak, že $|X| = i$ a libovolnou podmnožinu Y indexů sloupců matice A tak, že $|Y| = i$. Označme dále M matici tvaru $i \times i$, která vznikne z A vynecháním řádků neležících v X a sloupců neležících v Y.

Poté uvažujme matici B tvořenou sloupci matice $-A^T$ s indexy z množiny X a sloupci matice I_{n-k} s indexy z množiny $\{1, \ldots, n-k\} \backslash Y$. Jedná se o celkem $n-k$ sloupců prověrkové matice H, proto $\det(B) \neq 0$.

Potom existují $j, k \in \mathbb{N}$ taková, že

$$\det(M) = \det(M^T) = (-1)^j \det(-M^T) = (-1)^k \det(B) \neq 0.$$

První rovnost plyne z [[4], Tvrzení 7.18.] a třetí z Věty o rozvoji podle sloupce [[4], Věta 7.32]. Každá čtvercová podmatice A je tedy regulární.

□

Příklad. Pro znázornění průběhu důkazu provedeme postup na příkladu. Mějme

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} \\ a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} \\ a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} \end{pmatrix},$$

$$H = [-A^T|I_4] = \begin{pmatrix} -a_{1,1} & -a_{2,1} & -a_{3,1} & 1 & 0 & 0 & 0 \\ -a_{1,2} & -a_{2,2} & -a_{3,2} & 0 & 1 & 0 & 0 \\ -a_{1,3} & -a_{2,3} & -a_{3,3} & 0 & 0 & 1 & 0 \\ -a_{1,4} & -a_{2,4} & -a_{3,4} & 0 & 0 & 0 & 1 \end{pmatrix}$$

V implikaci $\Longleftarrow$ zvolíme $i = 2$. Vybereme například 1. a 3. sloupec z matice $-A^T$, 2. a 3. sloupec z matice I_4. Tedy

$$B = \begin{pmatrix} -a_{1,1} & -a_{3,1} & 0 & 0 \\ -a_{1,2} & -a_{3,2} & 1 & 0 \\ -a_{1,3} & -a_{3,3} & 0 & 1 \\ -a_{1,4} & -a_{3,4} & 0 & 0 \end{pmatrix}.$$

Po přeskládání

$$\det(B') = \begin{vmatrix} 1 & 0 & -a_{1,2} & -a_{3,2} \\ 0 & 1 & -a_{1,3} & -a_{3,3} \\ 0 & 0 & -a_{1,1} & -a_{3,1} \\ 0 & 0 & -a_{1,4} & -a_{3,4} \end{vmatrix} = \begin{vmatrix} -a_{1,1} & -a_{3,1} \\ -a_{1,4} & -a_{3,4} \end{vmatrix} = \det(M),$$

kde M je podmatice tvaru 2×2 matice $-A^T$.

V implikaci $\Longrightarrow$ máme $p = 3$, zvolíme $i = 2,\ X = \{1,2\}$ a $Y = \{2,4\}$.

Dostáváme tak matice

$$M = \begin{pmatrix} a_{1,2} & a_{1,4} \\ a_{2,2} & a_{2,4} \end{pmatrix} \text{ a } B = \begin{pmatrix} -a_{1,1} & -a_{2,1} & 1 & 0 \\ -a_{1,2} & -a_{2,2} & 0 & 0 \\ -a_{1,3} & -a_{2,3} & 0 & 1 \\ -a_{1,4} & -a_{2,4} & 0 & 0 \end{pmatrix}.$$

Potom

$$\det(M) = \begin{vmatrix} a_{1,2} & a_{1,4} \\ a_{2,2} & a_{2,4} \end{vmatrix} = (-1)^j \det(-M^T) = (-1)^j \begin{vmatrix} -a_{1,2} & -a_{2,2} \\ -a_{1,4} & -a_{2,4} \end{vmatrix} = (-1)^k \det(B)$$

Poznámka. V důkazu Věty 5 jsme použili, že přeskládání matice mění pouze znaménko jejího determinantu. Nad tělesy charakteristiky dva, kterými se budeme zabývat především, nemá prohazování řádků a sloupců matice na hodnotu jejího determinantu dokonce žádný vliv.

Tím dostáváme jako důležitý důsledek charakterizaci MDS matic. Jedná se o formulaci Věty 5 v řeči matic.

Důsledek 6. *Matice A je MDS právě tehdy, když je každá její čtvercová podmatice regulární.*

Z předchozího důsledku vyplývá následující ekvivalence.

Důsledek 7. *Čtvercová matice s prvky v tělese $\mathbb{F}$ je MDS právě tehdy, když je determinant každé její čtvercové podmatice nenulový. Speciálně MDS matice obsahují pouze nenulové prvky.*

Důsledek 8. *Čtvercová matice tvaru 2×2 nad tělesem $\mathbb{F}$ je MDS právě tehdy, když je regulární a neobsahuje nulové prvky tělesa $\mathbb{F}$.*

Lemma 9. [1, Lemma 1] *Buď A MDS matice nad tělesem $\mathbb{F}$. Potom je matice A' získaná přenásobením řádků nebo sloupců matice A libovolným $c \in \mathbb{F} \setminus \{0\}$, případně permutací řádků nebo sloupců, také MDS. Matice A je MDS právě tehdy, když A^T je MDS.*

Důkaz: Přenásobení libovolného sloupce nebo řádku matice A nenulovým prvkem tělesa, jejich permutace, ani transpozice matice A nezmění regularitu resp. singularitu jejích čtvercových podmatic.

□

1.2 Cirkulantní matice

Cirkulantní matice mají jednoduchou strukturu. Jsou definovány jediným vektorem, prvním řádkem matice. Další řádky jsou vždy cyklickým posunutím předchozího řádku o jednu pozici doprava. V této sekci je čerpáno ze skript konečných těles [5].

Definice 7 (Cirkulantní matice)**.** *Matice*

$$\mathrm{Circ}(a_0, a_1, a_2 \ldots, a_{d-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{d-1} \\ a_{d-1} & a_0 & a_1 & \ldots & a_{d-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{pmatrix}$$

tvaru $d \times d$ nad tělesem $\mathbb{F}$ se nazývá cirkulantní*.*

Lemma 10. *Lineární kombinace cirkulantních matic stejného tvaru nad stejným tělesem je cirkulantní matice téhož tvaru.*

Důkaz: Nechť $A = \mathrm{Circ}(a_0, \ldots, a_{d-1})$ a $B = \mathrm{Circ}(b_0, \ldots, b_{d-1})$ jsou cirkulantní matice tvaru $d \times d$ nad tělesem $\mathbb{F}$, potom zřejmě

$$A + B = \mathrm{Circ}(a_0 + b_0, \ldots, a_{d-1} + b_{d-1})$$

je cirkulantní matice. Díky indukci je rovněž součet konečně mnoha cirkulantních matic stejného tvaru nad stejným tělesem cirkulantní matice. Zároveň pro libovolné $c \in \mathbb{F}$ zřejmě platí

$$c \cdot \mathrm{Circ}(a_0, \ldots, a_{d-1}) = \mathrm{Circ}(c \cdot a_0, \ldots, c \cdot a_{d-1})$$

a cirkulantní matice jsou tak uzavřeny na násobení skalárem. Tím dostáváme lemma.

□

Příklad. Lineární kombinace cirkulantních matic tvaru 3×3 nad tělesem $\mathbb{F}_5$:

$$3 \cdot \mathrm{Circ}(1,0,4) + 2 \cdot \mathrm{Circ}(0,2,3) + 2 \cdot I_3 = 3 \cdot \begin{pmatrix} 1 & 0 & 4 \\ 4 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix} + 2 \cdot \begin{pmatrix} 0 & 2 & 3 \\ 3 & 0 & 2 \\ 2 & 3 & 0 \end{pmatrix} + 2 \cdot I_3 =$$

$$= \begin{pmatrix} 3 & 0 & 2 \\ 2 & 3 & 0 \\ 0 & 2 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 4 & 1 \\ 1 & 0 & 4 \\ 4 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 4 & 3 \\ 3 & 0 & 4 \\ 4 & 3 & 0 \end{pmatrix} = \mathrm{Circ}(0,4,3)$$

Nyní uvedeme důležité lemma, které charakterizuje cirkulantní matice. Každá cirkulantní matice je totiž lineární kombinací jistých permutačních matic P^i.

Lemma 11. [1, Proposition 1] *Matice A tvaru $d \times d$ nad tělesem $\mathbb{F}$ je cirkulantní matice rovná* $\mathrm{Circ}(a_0, \ldots, a_{d-1})$ *právě tehdy, když je možné zapsat ji ve tvaru*

$$A = a_0 I_d + a_1 P + a_2 P^2 + \cdots + a_{d-1} P^{d-1},$$

kde $P = \mathrm{Circ}(0, 1, 0, \ldots, 0)$, $a_i \in \mathbb{F}$ *pro* $i = 0, \ldots, d-1$ *a* I_d *je jednotková matice tvaru* $d \times d$.

Důkaz: Buď $P = \mathrm{Circ}(0, 1, 0, \ldots, 0)$ matice tvaru $d \times d$, tedy

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Matici P je možné po sloupcích rozepsat jako $P = (\mathbf{e}_d|\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_{d-1})$, kde $\mathbf{e}_i$ je $i-$tý vektor kanonické báze. Jejím mocněním dochází pouze k permutaci sloupců. Dokážeme, že platí následující rovnost: $P^i = (\mathbf{e}_{d-i+1}|\mathbf{e}_{d-i+2}|\cdots|\mathbf{e}_d|\mathbf{e}_1|\cdots|\mathbf{e}_{d-i})$, kde indexy uvažujeme modulo d z množiny $\{1, \ldots, d\}$. Postupujme indukcí dle i:

- $i = 1 : P^1 = (\mathbf{e}_d|\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_{d-1}) = P$
- $i \to i+1$: Ze sloupcového pohledu na násobení matic dostaneme

$$\begin{aligned} P^{i+1} = P^i P =& (\mathbf{e}_{d-i+1}|\mathbf{e}_{d-i+2}|\cdots|\mathbf{e}_d|\mathbf{e}_1|\ldots|\mathbf{e}_{d-i})(\mathbf{e}_d|\mathbf{e}_1|\mathbf{e}_2|\cdots|\mathbf{e}_{d-1}) \\ =& (\mathbf{e}_{d-i}|\mathbf{e}_{d-i+1}|\cdots|\mathbf{e}_d|\mathbf{e}_1|\ldots|\mathbf{e}_{d-i-1}) \\ =& (\mathbf{e}_{d-(i+1)+1}|\mathbf{e}_{d-(i+1)+2}|\cdots|\mathbf{e}_d|\mathbf{e}_1|\ldots|\mathbf{e}_{d-(i+1)}). \end{aligned}$$

Tedy platí $P^i = \mathrm{Circ}(0, \ldots, 0, 1, 0, \ldots, 0) = \mathrm{Circ}(\mathbf{e}_{i+1}^T)$.

$\Longleftarrow$

Matice $a_i P^i$ je pro libovolné $i = 0, \ldots, d-1$ cirkulantní a platí

$$a_i P^i = \mathrm{Circ}(0, \ldots, 0, a_i, 0, \ldots, 0).$$

Součtem konečně mnoha cirkulantních matic je dle Lemmatu 10 cirkulantní matice a tedy matice $A = a_0 I_d + a_1 P + a_2 P^2 + \cdots + a_{d-1} P^{d-1}$ je také cirkulantní. Zřejmě platí $a_0 I_d + a_1 P + a_2 P^2 + \cdots + a_{d-1} P^{d-1} = \mathrm{Circ}(a_0, \ldots, a_{d-1})$, protože průnik nenulových pozic cirkulantních matic $a_i P^i$ je pro různá $i = 0, \ldots, d-1$ prázdný.

$\Longrightarrow$

Z rovnosti $P^i = \mathrm{Circ}(0, \ldots, 0, 1, 0, \ldots, 0) = \mathrm{Circ}(\mathbf{e}_{i+1}^T)$ již plyne, že

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{d-1} \\ a_{d-1} & a_0 & a_1 & \cdots & a_{d-2} \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{pmatrix} = a_0 I_d + a_1 P + \cdots + a_{d-1} P^{d-1}.$$

□

Poznámka. Z důkazu je zřejmé, že pro matici $P = \mathrm{Circ}(0, 1, 0, \ldots, 0)$ tvaru $d \times d$ pro libovolné $d \geq 1$ platí $P^d = I_d$.

Příklad. Uvažujme cirkulantní matici $\mathrm{Circ}(0, 4, 3)$ tvaru 3×3 nad tělesem $\mathbb{F}_5$, pak

$$\mathrm{Circ}(0,4,3) = \begin{pmatrix} 0 & 4 & 3 \\ 3 & 0 & 4 \\ 4 & 3 & 0 \end{pmatrix} = 0 \cdot I_3 + 4 \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + 3 \cdot \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = 0 \cdot I_3 + 4 \cdot P + 3 \cdot P^2.$$

Následující dvě lemmata vycházejí z [1, Lemma 2].

Lemma 12. *Transpozice cirkulantní matice* $A = \mathrm{Circ}(a_0, a_1, \ldots, a_{d-1})$ *je opět cirkulantní matice a platí* $A^T = \mathrm{Circ}(a_0, a_{d-1}, \ldots, a_1)$.

Důkaz: Transpozice cirkulantní matice je pouze zobrazení: $f_T : f_T(A) = TAT$, kde

$$T = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Pro cirkulantní matici A tedy platí

$$\begin{aligned} A^T = TAT &= T(a_0 I_d + a_1 P + a_2 P^2 + \cdots + a_{d-1} P^{d-1})T \\ &= a_0 T I_d T + a_1 TPT + a_2 TP^2T + \cdots + a_{d-1} TP^{d-1}T. \end{aligned}$$

Chceme dokázat, že pro libovolné $i = 0, \ldots, d-1$ platí $(P^i)^T = TP^iT = P^{d-i}$. Zvolme libovolné fixní d. Potom indukcí podle i:

- $i = 0 : (P^0)^T = (I_d)^T = I_d = P^d$
- $i \to i + 1$: Protože $T^{-1} = T$, platí

$$(P^{i+1})^T = TP^iPT = TP^iTTPT = P^{d-i}P^{d-1} = P^{2d-i-1} = P^{d-(i+1)}.$$

Potom $A^T = a_0 I_d + a_1 P^{d-1} + a_2 P^{d-2} + \cdots + a_{d-1} P^1 = \mathrm{Circ}(a_0, a_{d-1}, \ldots, a_1)$. □

Příklad. Transpozice

$$\mathrm{Circ}(0,4,3)^T = \begin{pmatrix} 0 & 4 & 3 \\ 3 & 0 & 4 \\ 4 & 3 & 0 \end{pmatrix}^T = \begin{pmatrix} 0 & 3 & 4 \\ 4 & 0 & 3 \\ 3 & 4 & 0 \end{pmatrix} = \mathrm{Circ}(0,3,4)$$

je opět cirkulantní matice.

Cirkulantní matice jsou také uzavřené na součin, ten je navíc komutativní.

Lemma 13. *Součin dvou cirkulantních matic tvaru $d \times d$ nad tělesem $\mathbb{F}$ je cirkulantní matice. Navíc pro dvě cirkulantní matice A, B tvaru $d \times d$ platí $AB = BA$.*

Důkaz: Využitím Lemmatu 11 můžeme cirkulantní matice rozepsat. Pro cirkulantní matice

$$A = a_0 I_d + a_1 P + \cdots + a_{d-1} P^{d-1}$$

a

$$B = b_0 I_d + b_1 P + \cdots + b_{d-1} P^{d-1},$$

kde $P = \mathrm{Circ}(0, 1, 0, \ldots, 0)$ je permutační matice tvaru $d \times d$ platí

$$AB = a_0 b_0 I_d + (a_1 b_0 + a_0 b_1) P + \cdots + (a_{d-1} b_{d-1}) P^{2d-2},$$

kde mocninu permutační matice díky poznámce za Lemmatem 11 můžeme brát modulo d. Tedy

$$AB = c_0 I_d + c_1 P + \cdots + c_{d-1} P^{d-1} = \mathrm{Circ}(c_0, \ldots, c_{d-1})$$

pro nějaká $c_0, \ldots, c_{d-1}$ z příslušného tělesa.
Protože platí $P^i \cdot P^j = P^{i+j} = P^{j+i} = P^j \cdot P^i$, dostáváme $AB = BA$.

□

Indukcí dostáváme následující důsledek.

Důsledek 14. *Součin konečně mnoha cirkulantních matic stejného tvaru nad stejným tělesem je cirkulantní matice.*

Příklad. Vynásobíme cirkulantní matice $\mathrm{Circ}(0, 3, 4)$ a $\mathrm{Circ}(1, 2, 3)$ tvaru 3×3 nad tělesem $\mathbb{F}_5$:

$$\mathrm{Circ}(0,3,4) \cdot \mathrm{Circ}(1,2,3) = \begin{pmatrix} 0 & 3 & 4 \\ 4 & 0 & 3 \\ 3 & 4 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} =$$

$$\mathrm{Circ}(2,0,0) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 3 & 4 \\ 4 & 0 & 3 \\ 3 & 4 & 0 \end{pmatrix} = \mathrm{Circ}(1,2,3) \cdot \mathrm{Circ}(0,3,4).$$

Již jsme dokázali, že cirkulantní matice stejného tvaru $d \times d$ nad stejným tělesem $\mathbb{F}$ jsou uzavřené na lineární kombinace, transpozice i součin, který je navíc komutativní. Tím pádem takovéto cirkulantní matice tvoří jistou strukturu, takzvanou komutativní algebru, tedy komutativní okruh a zároveň vektorový prostor nad tělesem $\mathbb{F}$.

Lemma 15. *Cirkulantní matice tvaru $d \times d$ nad tělesem $\mathbb{F}$ tvoří komutativní algebru s bází $P^0, \ldots, P^{d-1}$ vektorového prostoru nad tímto tělesem.*

Důkaz: Z lineární algebry víme, že čtvercové matice stejného tvaru nad stejným tělesem tvoří vektorový prostor. Z algebry víme, že tyto matice tvoří rovněž okruh. Dokážeme, že cirkulantní matice stejného tvaru $d \times d$ tvoří komutativní podalgebru nekomutativní algebry matic tvaru $d \times d$, tedy neprázdnou podmnožinu okruhu uzavřenou na sčítání a násobení skalárem z tělesa $\mathbb{F}$ (charakterizace podprostoru) a na násobení matic (spolu se sčítáním charakterizace podokruhu).

Že se jedná o neprázdnou podmnožinu matic téhož tvaru je zřejmé. Dále z Lemmatu 10 dostáváme uzavřenost na lineární kombinace, tedy na součet a násobení skalárem z tělesa $\mathbb{F}$. Z Lemmatu 13 dostáváme uzavřenost na násobení a jeho komutativitu. Z Lemmatu 11 víme, že každou cirkulantní matici tvaru $d \times d$ lze zapsat jako lineární kombinaci $P^0, \ldots, P^{d-1}$, což je lineárně nezávislá posloupnost nad tělesem $\mathbb{F}$. Tím je tvrzení dokázáno.

□

Lemmatem 15 jsme jasně určili strukturu cirkulantních matic tvaru $d \times d$ nad tělesem $\mathbb{F}$. Tuto strukturu je možné reprezentovat pomocí polynomů stupně menšího než d nad tímto tělesem.

Lemma 16. *Komutativní algebra cirkulantních matic tvaru $d \times d$ nad tělesem $\mathbb{F}$ s bází $P^0, \ldots, P^{d-1}$ je izomorfní faktorové algebře $\mathbb{F}[x]/(x^d - 1)$.*

Důkaz: Označme $Circ_{(d)}$ algebru cirkulantních matic tvaru $d \times d$. Uvažujme zobrazení $\Phi : \mathbb{F}[x] \to Circ_{(d)}$, které prvku $f = \sum_{i=0}^{\deg(f)} a_i x^i$ přiřadí prvek $\sum_{i=0}^{\deg(f)} a_i P^i$. Mějme libovolné dva polynomy $f = \sum_{i=0}^{\deg(f)} a_i x^i, g = \sum_{i=0}^{\deg(g)} b_i x^i \in \mathbb{F}[x]$, pak platí:

$$\Phi(1) = \Phi(x^0) = P^0 = I_d$$

$$\Phi(c \cdot f) = \Phi\left(\sum_{i=0}^{\deg(f)} c \cdot a_i x^i \right) = \sum_{i=0}^{\deg(f)} c \cdot a_i P^i =$$

$$= c \cdot \sum_{i=0}^{\deg(f)} a_i P^i = c \cdot \Phi\left(\sum_{i=0}^{\deg(f)} a_i x^i \right) = c \cdot \Phi(f),$$

pro libovolný skalár $c \in \mathbb{F}$. Dále platí

$$\Phi(f) + \Phi(g) = \Phi\left(\sum_{i=0}^{\deg(f)} a_i x^i \right) + \Phi\left(\sum_{i=0}^{\deg(g)} b_i x^i \right) = \sum_{i=0}^{\deg(f)} a_i P^i + \sum_{i=0}^{\deg(g)} b_i P^i =$$

$$= \sum_{i=0}^{\max(\deg(f),\, \deg(g))} (a_i + b_i) P^i = \Phi\left(\sum_{i=0}^{\max(\deg(f),\, \deg(g))} (a_i + b_i) x^i \right) = \Phi(f + g),$$

kde pro $i > \deg(f)$ definujeme $a_i = 0$ a pro $i > \deg(g)$ definujeme $b_i = 0$.
Zároveň

$$\Phi(f) \cdot \Phi(g) = \Phi\left(\sum_{i=0}^{\deg(f)} a_i x^i \right) \cdot \Phi\left(\sum_{i=0}^{\deg(g)} b_i x^i \right) = \left(\sum_{i=0}^{\deg(f)} a_i P^i \right) \cdot \left(\sum_{i=0}^{\deg(g)} b_i P^i \right) =$$

$$= \sum_{i=0}^{\deg(f)+\deg(g)} \left(\sum_{j=0}^{i} (a_j b_{i-j}) \right) P^i = \Phi\left(\sum_{i=0}^{\deg(f)+\deg(g)} \left(\sum_{j=0}^{i} (a_j b_{i-j}) \right) x^i \right) = \Phi(f \cdot g),$$

kde opět pro $i > \deg(f)$ definujeme $a_i = 0$ a pro $i > \deg(g)$ definujeme $b_i = 0$. Zobrazení Φ je tedy homomorfismus.

S využitím vlastnosti $P^d = I_d$ dokážeme, že jádro zobrazení Φ je rovno ideálu $(x^d - 1)$. Z rovnosti $P^d = I_d$ plyne, že $x^d - 1 \in \mathrm{Ker}(\Phi)$, tedy $(x^d - 1) \subset \mathrm{Ker}(\Phi)$, protože $\mathrm{Ker}(\Phi)$ je ideál. Naopak uvažujme polynom $f \in \mathrm{Ker}(\Phi)$. V eukleidovském oboru $\mathbb{F}[x]$ je možné polynomy jednoznačně dělit se zbytkem, tím získáme rovnost

$$f \;=\; q(x^d - 1) + r,$$

kde $q, r \in \mathbb{F}[x]$ a $\deg(r) < d$. Jelikož $f \in \mathrm{Ker}(\Phi)$ a $q(x^d - 1) \in \mathrm{Ker}(\Phi)$, také $r \in \mathrm{Ker}(\Phi)$. Matice $P^0, ..., P^{d-1}$ tvoří bázi všech cirkulantních matic tvaru $d \times d$ nad tělesem $\mathbb{F}$, r je tedy roven nulovému polynomu a $f \in (x^d - 1)$. Dostáváme tak $\mathrm{Ker}(\Phi) \subset (x^d - 1)$. Dohromady $\mathrm{Ker}(\Phi) = (x^d - 1)$.

Zobrazení Φ je tak homomorfismus okruhu polynomů $\mathbb{F}[x]$ na algebru cirkulantních matic $Circ_{(d)}$ s jádrem $(x^d - 1)$. Podle první věty o izomorfismu je pak $Circ_{(d)}$ izomorfní $\mathbb{F}[x]/(x^d - 1)$.

□

Příklad. Cirkulantní matici $\mathrm{Circ}(0, 3, 4)$ tvaru 3×3 nad tělesem $\mathbb{F}_5$ můžeme reprezentovat jako polynom následujícím způsobem:

$$\mathrm{Circ}(0,3,4) = \begin{pmatrix} 0 & 3 & 4 \\ 4 & 0 & 3 \\ 3 & 4 & 0 \end{pmatrix} = 0 \cdot I_3 + 3 \cdot P + 4 \cdot P^2 \approx 3x + 4x^2.$$

Součin i součet cirkulantních matic potom odpovídá těmto operacím nad faktorovou algebrou $\mathbb{F}_5[x]/(x^3 - 1)$.

$$\begin{aligned} &2 \cdot \mathrm{Circ}(0,3,4) \cdot \mathrm{Circ}(1,2,3) + 3 \cdot \mathrm{Circ}(1,0,4) = \\ &= 2 \cdot \begin{pmatrix} 0 & 3 & 4 \\ 4 & 0 & 3 \\ 3 & 4 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} + 3 \cdot \begin{pmatrix} 1 & 0 & 4 \\ 4 & 1 & 0 \\ 0 & 4 & 1 \end{pmatrix} = \\ &= 2 \cdot \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} 3 & 0 & 2 \\ 2 & 3 & 0 \\ 0 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 2 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix} = \mathrm{Circ}(2,0,2) \end{aligned}$$

Zároveň však můžeme počítat s polynomy.

$$2 \cdot (3x + 4x^2) \cdot (1 + 2x + 3x^2) + 3 \cdot (1 + 4x^2) = 2 \cdot (2x^4 + 2x^3 + 3x) + 3 + 2x^2 =$$

$$= 4x + 4 + x + 3 + 2x^2 = 2 + 2x^2 \approx \mathrm{Circ}(2,0,2)$$

Ve zbytku sekce budeme pracovat nad konečným tělesem $\mathbb{F}_q$, především pak nad $\mathbb{F}_{2^n}$. To nám umožní formulovat silnější tvrzení na základě použití charakteristiky tělesa. Odvodíme explicitní vzorec pro výpočet determinantu cirkulantní matice tvaru $2^d \times 2^d$ nad tímto tělesem, který v následující kapitole použijeme při konstrukci MDS matic.

Lemma 17. *Buď M regulární cirkulantní matice tvaru $d \times d$ nad konečným tělesem $\mathbb{F}_q$, potom je M^{-1} také cirkulantní matice tvaru $d \times d$.*

Důkaz: Nad konečným tělesem $\mathbb{F}_q$ existuje pouze konečně mnoho matic tvaru $d \times d$, musí tedy existovat $n \in \mathbb{N}$ takové, že $MM^{n-1} = M^n = I_d$, potom $M^{-1} = M^{n-1}$. Protože je M^{-1} součinem $n-1$ stejných cirkulantních matic, z Důsledku 14 lemmatu o součinu cirkulantních matic víme, že M^{-1} je rovněž cirkulantní matice.

□

Poznámka. Lemma 17 platí rovněž pro nekonečné těleso $\mathbb{F}$. Cirkulantnost inverzní matice je možné dokázat přes Cayley-Hamiltonovu větu [4, Věta 9.119] rozepsáním v bázi $P^0, P^1, \ldots, P^{d-1}$.

Poznámka. Na komutativních okruzích R charakteristiky p, speciálně pak na konečných tělesech $\mathbb{F}_{p^n}$ můžeme definovat význačné zobrazení $\sigma : R \to R$ definované předpisem $\sigma(a) = a^p$ pro každé $a \in R$. Jedná se o homomorfismus, takzvaný Frobeniův endomorfismus. Z konečných těles [5, Tvrzení 3.9] víme, že pro konečná tělesa $\mathbb{F}_{p^n}$ charakteristiky p je tento endomorfismus zároveň bijektivní, jedná se tak o Frobeniův automorfismus $\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ definovaný předpisem $\sigma(a) = a^p$.

Lemma 18. [1, Lemma 4] *Pro matici* $\mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1})$ *tvaru* $2^d \times 2^d$ *s prvky* $a_0, \ldots, a_{2^d-1} \in \mathbb{F}_{2^n}$ *platí* $\mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1})^{2^d} = (\sum_{i=0}^{2^d-1} a_i^{2^d}) I_{2^d}$.

Důkaz: Podle Lemmatu 11 platí

$$\mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1}) = a_0 I_{2^d} + a_1 P + a_2 P^2 + \cdots + a_{2^d-1} P^{2^d-1},$$

kde $P = \mathrm{Circ}(0, 1, 0, \ldots, 0)$ je tvaru $2^d \times 2^d$. Tedy

$$\mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1})^{2^d} = (a_0 I_{2^d} + a_1 P + a_2 P^2 + \cdots + a_{2^d-1} P^{2^d-1})^{2^d}.$$

Podle Lemmatu 15 tvoří cirkulantní matice tvaru $2^d \times 2^d$ komutativní okruh. Těleso $\mathbb{F}_{2^n}$ má charakteristiku 2. Z poznámky o Frobeniově endomorfismu tak víme, že mocnění na druhou, tedy také mocnění na 2^d, je homomorfismus.

$$(a_0 I_{2^d} + a_1 P + a_2 P^2 + \cdots + a_{2^d-1} P^{2^d-1})^{2^d} =$$
$$= (a_0 I_{2^d})^{2^d} + (a_1 P)^{2^d} + (a_2 P^2)^{2^d} + \cdots + (a_{2^d-1} P^{2^d-1})^{2^d}.$$

Tento výraz dále upravíme s využitím $P^{2^d} = I_{2^d}$ a dostaneme

$$(a_0 I_{2^d})^{2^d} + (a_1 P)^{2^d} + (a_2 P^2)^{2^d} + \cdots + (a_{2^d-1} P^{2^d-1})^{2^d} =$$
$$= a_0^{2^d} I_{2^d}^{2^d} + a_1^{2^d} P^{2^d} + a_2^{2^d} (P^2)^{2^d} + \cdots + a_{2^d-1}^{2^d} (P^{2^d-1})^{2^d} =$$
$$= a_0^{2^d} I_{2^d}^{2^d} + a_1^{2^d} P^{2^d} + a_2^{2^d} (P^{2^d})^2 + \cdots + a_{2^d-1}^{2^d} (P^{2^d})^{2^d-1} =$$
$$= a_0^{2^d} I_{2^d} + a_1^{2^d} I_{2^d} + a_2^{2^d} (I_{2^d})^2 + \cdots + a_{2^d-1}^{2^d} (I_{2^d})^{2^d-1} =$$
$$= a_0^{2^d} I_{2^d} + a_1^{2^d} I_{2^d} + a_2^{2^d} I_{2^d} + \cdots + a_{2^d-1}^{2^d} I_{2^d} =$$
$$= \left(\sum_{i=0}^{2^d-1} a_i^{2^d} \right) I_{2^d}.$$

□

Příklad. Pokud cirkulantní matici $\mathrm{Circ}(\alpha, 1+\alpha, 1, 1)$ tvaru 4×4 nad tělesem $\mathbb{F}_4 = {}^{\mathbb{F}_2[\alpha]}\!/_{(\alpha^2+\alpha+1)}$ umocníme na čtvrtou, získáme jednotkovou matici I_4, protože

$$\alpha^4 + (1+\alpha)^4 + 1 + 1 = \alpha^4 + 1^4 + \alpha^4 + 1 + 1 = 1,$$

kde v první rovnosti využíváme Frobeniův automorfismus tělesa $\mathbb{F}_4$. Dostáváme tak rovnost

$$\begin{pmatrix} \alpha & 1+\alpha & 1 & 1 \\ 1 & \alpha & 1+\alpha & 1 \\ 1 & 1 & \alpha & 1+\alpha \\ 1+\alpha & 1 & 1 & \alpha \end{pmatrix}^4 = I_4.$$

Pokud tedy cirkulantní matici tvaru $2^d \times 2^d$ s prvky z tělesa charakteristiky 2 umocníme na 2^d, získáme podle Lemmatu 18 diagonální matici. U takovýchto matic je velmi jednoduché spočítat determinant.

Tvrzení 19 (Determinant cirkulantní matice)**.** [1, Corollary 1] *Platí*

$$\det(\mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1})) = \sum_{i=0}^{2^d-1} a_i^{2^d},$$

kde $a_0, \ldots, a_{2^d-1} \in \mathbb{F}_{2^n}$.

Důkaz: Označme $A = \mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1})$. Z lineární algebry [4, Věta 7.26] víme, že determinant součinu matic je roven součinu jejich determinantů, tedy

$$\det(A^{2^d}) = \det(\underbrace{AA\ldots AA}_{2^d\text{-krát}}) = \underbrace{\det(A)\det(A)\ldots\det(A)\det(A)}_{2^d\text{-krát}} = (\det(A))^{2^d}.$$

Z Lemmatu 18 víme, že platí $A^{2^d} = (\sum_{i=0}^{2^d-1} a_i^{2^d}) I_{2^d}$, tedy

$$(\det(A))^{2^d} = \det(A^{2^d}) = \det((\sum_{i=0}^{2^d-1} a_i^{2^d}) I_{2^d}) = (\sum_{i=0}^{2^d-1} a_i^{2^d})^{2^d},$$

protože determinant diagonální matice I_{2^d} je jen součinem 2^d prvků na diagonále.

Z rovnosti obrazů $(\det(A))^{2^d} = (\sum_{i=0}^{2^d-1} a_i^{2^d})^{2^d}$ plyne díky Frobeniově automorfismu rovnost vzorů $(\det(A))^{2^{d-1}} = (\sum_{i=0}^{2^d-1} a_i^{2^d})^{2^{d-1}}$. Takto lze postupovat až dostaneme $\det(A) = \sum_{i=0}^{2^d-1} a_i^{2^d}$.

□

Příklad. Determinant matice $\mathrm{Circ}(\alpha, 1+\alpha, 1, 1)$ nad $\mathbb{F}_4 = {}^{\mathbb{F}_2[\alpha]}\!/_{(\alpha^2+\alpha+1)}$ je roven

$$\alpha^4 + (1+\alpha)^4 + 1 + 1 = 1.$$

1.3 Biregulární matice

Další skupinou matic, která nám pomůže při konstrukci MDS matic, jsou takzvané biregulární matice. Jedná se o matice, které mají v řádcích i sloupcích v jistém smyslu rozmanité prvky. Ukážeme, že každá MDS matice musí být biregulární a stanovíme podmínky, jež musí každá cirkulantní MDS matice tvaru 4×4 nad tělesem $\mathbb{F}$ splňovat. Sekce je inspirována článkem [6].

Definice 8 (Biregulární matice)**.** *Nechť $\mathbb{F}^*$ je multiplikativní grupa tělesa $\mathbb{F}$.*

1. Matice tvaru 2×2 s hodnotami z $\mathbb{F}^*$ se nazývá biregulární*, jestliže alespoň jeden řádek a jeden sloupec obsahují dvě různé hodnoty.*

2. Matice tvaru $s \times t$ s hodnotami z $\mathbb{F}^*$ se nazývá biregulární*, jestliže je každá její čtvercová podmatice tvaru 2×2 biregulární.*

Poznámka. Obvykle se biregulární matice definují pro konečná tělesa $\mathbb{F}_q$.

Příklad. Biregulární maticí nad tělesem $\mathbb{F}_5$ je například matice

$$\begin{pmatrix} 1 & 2 & 1 & 3 \\ 1 & 4 & 2 & 2 \\ 3 & 4 & 4 & 3 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

jelikož neobsahuje žádnou čtvercovou podmatici tvaru 2×2, která by měla oba sloupce nebo řádky stejné.

Z charakterizace MDS matic pomocí regularity jejich podmatic plyne následující tvrzení.

Tvrzení 20. *Každá MDS matice tvaru alespoň 2×2 nad tělesem $\mathbb{F}$ je biregulární.*

Důkaz: Čtvercová matice tvaru alespoň 2×2, která není biregulární, obsahuje podmatici tvaru 2×2, jež má v obou sloupcích nebo řádcích stejné hodnoty. Obsahuje tedy podmatici:

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix} \text{ nebo } \begin{pmatrix} a & b \\ a & b \end{pmatrix},$$

kde $a, b \in \mathbb{F}$ nejsou nutně různé. Determinant těchto podmatic je v obou případech nulový. Matice tak nemůže být dle Důsledku 7 MDS.

□

Opačná implikace ale neplatí. Příkladem biregulární matice, která není MDS, je třeba následující matice nad tělesem $\mathbb{F}_5$.

$$M = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 1 \\ 3 & 1 & 4 \end{pmatrix}$$

Matice není MDS, protože $\det(M) = 0$, ale je biregulární, protože každý řádek i sloupec každé její podmatice tvaru 2×2 obsahuje dvě různé hodnoty.

Získané nástroje nám tak umožňují určit, jaké podmínky musí splňovat každá cirkulantní MDS matice tvaru 4×4 nad tělsem $\mathbb{F}$.

Tvrzení 21. *Cirkulantní matice $A = \mathrm{Circ}(a_0, a_1, a_2, a_3)$ tvaru 4×4 s prvky v $\mathbb{F}^*$ je biregulární právě tehdy, nastane-li jedna z následujících možností:*

1. *Hodnoty a_0, a_1, a_2, a_3 jsou po dvou různé.*
2. *Existuje právě jeden index $i \in \{0, 1, 2, 3\}$ takový, že $a_i = a_{i+1 \mod 4}$ a pro všechny indexy $j \neq i$ jsou hodnoty a_j po dvou různé.*

Důkaz: $\Longleftarrow$
V případě, že jsou hodnoty a_0, a_1, a_2, a_3 po dvou různé, je matice A zřejmě biregulární, protože rovněž hodnoty ve všech sloupcích jsou po dvou různé. Ve druhém případě uvedeného tvrzení můžeme BÚNO předpokládat, že $i = 0$, protože je matice cirkulantní. Máme tedy $a_0 = a_1$ a po dvou různé hodnoty a_1, a_2, a_3, matice A tedy vypadá následovně:

$$A = \begin{pmatrix} a_1 & a_1 & a_2 & a_3 \\ a_3 & a_1 & a_1 & a_2 \\ a_2 & a_3 & a_1 & a_1 \\ a_1 & a_2 & a_3 & a_1 \end{pmatrix}$$

a je zřejmě biregulární.
$\Longrightarrow$
Pro spor předpokládejme, že není splněna ani jedna z možností uvedených v tvrzení, potom nastane alespoň jedna z následujících dvou možností:

1. Existuje alespoň jeden index $i \in \{0, 1, 2, 3\}$ splňující $a_i = a_{i+2 \mod 4}$ nebo
2. Existují alespoň dva různé indexy $i, j \in \{0, 1, 2, 3\}$ splňující $a_i = a_{i+1 \mod 4}$ a $a_j = a_{j+1 \mod 4}$

Opět můžeme BÚNO předpokládat, že $i = 0$. V prvním případě matice A obsahuje podmatici B:

$$A = \begin{pmatrix} a_0 & a_1 & a_0 & a_3 \\ a_3 & a_0 & a_1 & a_0 \\ a_0 & a_3 & a_0 & a_1 \\ a_1 & a_0 & a_3 & a_0 \end{pmatrix}, \; B = \begin{pmatrix} a_0 & a_0 \\ a_0 & a_0 \end{pmatrix}$$

a zřejmě tak není biregulární. Ve druhém případě můžeme díky vlastnostem indexů i a j BÚNO uvažovat pouze dvě možnosti pro jejich vzdálenosti. Buďto $j = i + 1$ a tedy $a_0 = a_1 = a_2$, čímž nastává zároveň první možnost a matice A tak není biregulární, nebo $j = i + 2$, potom $a_0 = a_1$ a $a_2 = a_3$ a matice A tak obsahuje podmatici B:

$$A = \begin{pmatrix} a_0 & a_0 & a_2 & a_2 \\ a_2 & a_0 & a_0 & a_2 \\ a_2 & a_2 & a_0 & a_0 \\ a_0 & a_2 & a_2 & a_0 \end{pmatrix}, \; B = \begin{pmatrix} a_0 & a_2 \\ a_0 & a_2 \end{pmatrix}$$

a zřejmě tak není biregulární.

□

Každá MDS cirkulantní matice tvaru 4×4 nad libovolným tělesem $\mathbb{F}$ tak musí splňovat podmínky uvedené v tvrzení výše. Až na cyklický posun a přenásobení nenulovým prvkem tělesa tedy mohou existovat pouze dva typy cirkulantních MDS matic tvaru 4×4 nad tělesem $\mathbb{F}$ a to $\mathrm{Circ}(a, b, 1, 1)$ a $\mathrm{Circ}(1, a, b, c)$, kde $a, b, c, 1$ jsou po dvou různé nenulové prvky tělesa $\mathbb{F}$.

Poznámka. Toto tvrzení je navíc možné zobecnit na cirkulantní matice dalších tvarů. Více se o tom můžeme dočíst například v článku [6].

2. Konstrukce MDS matic

Tato kapitola se zabývá samotnou konstrukcí MDS matic. Vychází především z článků [1] a [7, str. 794-795]. Využívá také znalostí konečných těles [5].

Poznámka. Z Lemmatu 9 víme, že MDS vlastnost matice je invariantní vůči přenásobení libovolného řádku či sloupce nenulovým prvkem tělesa, libovolné permutaci řádků a sloupců i transpozici. Z Lemmat 10 a 12 víme, že cirkulantnost matice je invariantní vůči přenásobení matice libovolným (nenulovým) prvkem tělesa i transpozici. Zřejmě je invariantní také vůči cyklické permutaci sloupců a řádků:

$$\mathrm{Circ}(a_0, a_1, a_2 \ldots, a_{d-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{d-1} \\ a_{d-1} & a_0 & a_1 & \ldots & a_{d-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{pmatrix} \rightarrow$$

$$\rightarrow \begin{pmatrix} a_{0+r} & a_{1+r} & a_{2+r} & \ldots & a_{d-1+r} \\ a_{d-1+r} & a_{0+r} & a_{1+r} & \ldots & a_{d-2+r} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{2+r} & a_{3+r} & a_{4+r} & \ldots & a_{1+r} \\ a_{1+r} & a_{2+r} & a_{3+r} & \ldots & a_{0+r} \end{pmatrix} = \mathrm{Circ}(a_{0+r}, a_{1+r}, a_{1+r}, \ldots, a_{d-1+r}),$$

kde indexy bereme modulo d a $r = 0, \ldots, d-1$.

Pokud celou MDS cirkulantní matici vynásobíme nenulovým prvkem tělesa, transponujeme nebo sloupce či řádky cyklicky posuneme, získáme opět MDS cirkulantní matici. Díky tomu jedna MDS cirkulantní matice $A = \mathrm{Circ}(a_0, \ldots, a_{d-1})$ určuje celou třídu MDS cirkulantních matic.

Označme $\mathbb{S}_A$ množinu $\{c \cdot \mathrm{Circ}(a_{0+r}, a_{1+r}, \ldots, a_{d-1+r}) | \, r = 0, \ldots, d-1;\, c \in \mathbb{F}^*\}$ a $\mathbb{S}_{A^T}$ množinu $\{c \cdot \mathrm{Circ}(a_{0+r}, a_{d-1+r}, \ldots, a_{1+r}) | \, r = 0, \ldots, d-1;\, c \in \mathbb{F}^*\}$.

Potom je každá matice $M \in \mathbb{S}_A \bigcup \mathbb{S}_{A^T}$ také MDS cirkulantní maticí a množina $\mathbb{S}_{A \cup A^T} = \mathbb{S}_A \bigcup \mathbb{S}_{A^T}$ tvoří třídu MDS cirkulantních matic určenou maticí A.

Nejprve se zaměříme na konstrukci MDS cirkulantních matic nad konečnými tělesy $\mathbb{F}_{2^n}$ charakteristiky 2.

$\mathbb{F}_2[x]/(f(x))$ je pro ireducibilní polynom $f(x)$ stupně n nad tělesem $\mathbb{F}_2$ izomorfní tělesu $\mathbb{F}_{2^n}$. Těleso $\mathbb{F}_{2^n}$ lze tedy chápat jako rozšíření tělesa $\mathbb{F}_2$ určené nějakým ireducibilním polynomem stupně n. Prvky tělesa $\mathbb{F}_{2^n}$ tak můžeme reprezentovat jako polynomy stupně menšího než n nad tělesem $\mathbb{F}_2$.

2.1 3 × 3 MDS matice

Tvrzení 22. *$A = \mathrm{Circ}(\alpha, 1, 1)$ je cirkulantní MDS matice, kde $\alpha \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ pro všechna $n \geq 2$.*

Důkaz: Determinant matice A je roven

$$\det(A) = \begin{vmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix} = \alpha^3 + 1^3 + 1^3 - (\alpha \cdot 1^2 + \alpha \cdot 1^2 + \alpha \cdot 1^2)$$
$$= \alpha^3 + \alpha = \alpha(\alpha^2 + 1) = \alpha(\alpha + 1)^2.$$

Protože $\alpha \neq 0$ a $\alpha \neq 1$, je tento determinant nenulový. Čtvercové podmatice tvaru 2×2 mají svůj determinant rovný buď

$$\begin{vmatrix} \alpha & 1 \\ 1 & \alpha \end{vmatrix} = \alpha^2 - 1^2 = \alpha^2 + 1 = (\alpha + 1)^2,$$

nebo

$$\begin{vmatrix} 1 & \alpha \\ 1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ \alpha & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & \alpha \end{vmatrix} = \begin{vmatrix} \alpha & 1 \\ 1 & 1 \end{vmatrix} = \alpha + 1.$$

Determinanty podmatic jsou tedy také nenulové a matice A je podle Důsledku 7 MDS.

□

Poznámka. V původnm článku [1, Proposition 2] je Tvrzení 22 uvedeno v následujícím znění:

$A = \mathrm{Circ}(\alpha, 1, 1)$ je cirkulantní MDS matice pro všechna $n \geq 2$, kde α je kořen generujícího polynomu $\mathbb{F}_{2^n}$.

Generujícím polynomem tělesa $\mathbb{F}_{2^n}$ je zde myšlen libovolný ireducibilní polynom $f(x) \in \mathbb{F}_2[x]$ stupně n.

Poznámka. Podle Tvrzení 22 dostáváme, že matice

$$A = \begin{pmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{pmatrix},$$

kde $\alpha \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ a $n \geq 2$, je MDS. Podle poznámky na začátku kapitoly tak určuje celou třídu MDS cirkulantních matic $\mathbb{S}_{A \cup A^T}$ obsahující matice

$$\begin{pmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{pmatrix}, \begin{pmatrix} 1 & \alpha & 1 \\ 1 & 1 & \alpha \\ \alpha & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & \alpha \\ \alpha & 1 & 1 \\ 1 & \alpha & 1 \end{pmatrix},$$

a všechny jejich nenulové násobky.

2.2 4×4 MDS matice

U matic tvaru 3×3 nám stačilo použít libovolný prvek $\alpha \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, u matic tvaru 4×4 jsou požadovány silnější podmínky.

Tvrzení 23. [1, Proposition 3] $A = \mathrm{Circ}(\alpha, 1+\alpha, 1, 1)$ *je cirkulantní MDS matice pro všechna* $\alpha \in \mathbb{F}_{2^n}$ *taková, že minimální polynom* α *nad tělesem* $\mathbb{F}_2$ *je stupně* $n \geq 4$.

Důkaz: Podle Tvrzení 19 platí $\det(\mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1})) = (\sum_{i=0}^{2^d-1} a_i^{2^d})$ a tedy

$$\begin{aligned}\det(A) &= \begin{vmatrix} \alpha & 1+\alpha & 1 & 1 \\ 1 & \alpha & 1+\alpha & 1 \\ 1 & 1 & \alpha & 1+\alpha \\ 1+\alpha & 1 & 1 & \alpha \end{vmatrix} \\ &= \alpha^4 + (1+\alpha)^4 + 1^4 + 1^4 = \alpha^4 + 1^4 + \alpha^4 + 0 = 1\end{aligned}$$

Protože je v tělesech charakteristiky dva sčítání a odčítání ekvivalentní operací a matice A je cirkulantní, je poměrně jednoduché spočítat determinanty všech jejích podmatic (tzv. minory).

Z Lemmatu 17 víme, že inverzní matice k matici A je opět cirkulantní, z lineární algebry [4, Věta 7.38] víme, že $A^{-1} = (\det(A))^{-1} \cdot \mathrm{Adj}(A)$, kde $\mathrm{Adj}(A)$ značí matici adjungovanou k matici A, tj. matici transponovanou k matici tvořené až na znaménko determinanty podmatic tvaru 3×3 matice A. Jelikož jsme v tělese charakteristiky dva, znaménka nehrají roli. Získáme tak pouze čtyři různé determinaty podmatic tvaru 3×3 matice A.

Zvolme $j = 0, \ldots, 3$, potom pro všechna $i = 0, \ldots, 3$ mají všechny podmatice tvaru 3×3 matice A tvořené výběrem všech krom i-tého řádku a všech krom $(i+j)$-tého sloupce (počítáno modulo 4) stejný determinant.

Pro $j = 0$ platí:

$$\begin{aligned}\begin{vmatrix} \alpha & 1+\alpha & 1 \\ 1 & \alpha & 1+\alpha \\ 1 & 1 & \alpha \end{vmatrix} &= \alpha^3 + (1+\alpha)^2 + 1 + \alpha + \alpha(1+\alpha) + \alpha(1+\alpha) \\ &= \alpha^3 + \alpha^2 + 1 + 1 + \alpha = \alpha^3 + \alpha^2 + \alpha.\end{aligned}$$

Pro $j = 1$ máme:

$$\begin{aligned}\begin{vmatrix} 1 & 1+\alpha & 1 \\ 1 & \alpha & 1+\alpha \\ 1+\alpha & 1 & \alpha \end{vmatrix} &= \alpha^2 + (1+\alpha)^3 + 1 + \alpha(1+\alpha) + (1+\alpha) + \alpha(1+\alpha) \\ &= \alpha^2 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha = \alpha^3 + 1.\end{aligned}$$

Obdobně dostaneme, že pro $j = 2$ je determinant podmatic roven

$$\begin{aligned}\begin{vmatrix} 1 & \alpha & 1 \\ 1 & 1 & 1+\alpha \\ 1+\alpha & 1 & \alpha \end{vmatrix} &= \alpha + 1 + \alpha(1+\alpha)^2 + (1+\alpha) + (1+\alpha) + \alpha^2 \\ &= \alpha + 1 + \alpha + \alpha^3 + \alpha^2 = \alpha^3 + \alpha^2 + 1.\end{aligned}$$

A stejně tak pro $j = 3$ můžeme spočítat, že determinant podmatic je roven

$$\begin{aligned}\begin{vmatrix} 1 & \alpha & 1+\alpha \\ 1 & 1 & \alpha \\ 1+\alpha & 1 & 1 \end{vmatrix} &= 1 + (1+\alpha) + \alpha^2(1+\alpha) + (1+\alpha)^2 + \alpha + \alpha \\ &= \alpha + \alpha^2 + \alpha^3 + (1+\alpha)^2 = \alpha^3 + \alpha + 1.\end{aligned}$$

Determinanty podmatic tvaru 3×3 jsou tedy následující:

$$\alpha^3 + \alpha^2 + \alpha, \alpha^3 + 1, \alpha^3 + \alpha^2 + 1 \text{ a } \alpha^3 + \alpha + 1.$$

Žádný z těchto determinantů není roven 0, protože minimální polynom α je stupně $n \geq 4$ a tyto polynomy mají všechny stupeň 3.

Pro podmatice tvaru 2×2 můžeme postupovat stejně, tj. spočítat, že determinanty těchto podmatic vyjdou

$$1, \alpha, 1+\alpha, \alpha^2, 1+\alpha^2, \alpha+\alpha^2 \text{ a } 1+\alpha+\alpha^2.$$

Žádný z těchto determinantů není roven 0, protože minimální polynom α je stupně $n \geq 4$ a tyto polynomy mají stupeň nejvýše 2.

Matice A obsahuje pouze nenulové prvky.

Determinanty všech podmatic jsou nenulové a matice A je podle Důsledku 7 MDS.

□

Poznámka. Pro $\alpha \in \mathbb{F}_{2^n}$ takové, že minimální polynom α je stupně $n \geq 4$, dostáváme celou třídu MDS cirkulantních matic $\mathbb{S}_{A \cup A^T}$ určenou maticí

$$A = \mathrm{Circ}(\alpha, 1+\alpha, 1, 1) = \begin{pmatrix} \alpha & 1+\alpha & 1 & 1 \\ 1 & \alpha & 1+\alpha & 1 \\ 1 & 1 & \alpha & 1+\alpha \\ 1+\alpha & 1 & 1 & \alpha \end{pmatrix}.$$

$\mathbb{S}_{A \cup A^T} = \mathbb{S}_A \bigcup \mathbb{S}_{A^T}$ obsahuje vedle matice $A = \mathrm{Circ}(\alpha, 1+\alpha, 1, 1)$ také matice

$$\mathrm{Circ}(1, \alpha, 1+\alpha, 1), \mathrm{Circ}(1, 1, \alpha, 1+\alpha), \mathrm{Circ}(1+\alpha, 1, 1, \alpha),$$

jejich transpozice, tedy matice

$$\mathrm{Circ}(\alpha, 1, 1, 1+\alpha), \mathrm{Circ}(1, 1, 1+\alpha, \alpha), \mathrm{Circ}(1, 1+\alpha, \alpha, 1), \mathrm{Circ}(1+\alpha, \alpha, 1, 1)$$

a nenulové násobky všech osmi výše uvedených matic.

V kryptografii je obvykle požadováno, aby matice obsahovala co nejvíce jednotek a šifrování pomocí ní tak nestálo mnoho času, nenulové násobky výše uvedených matic tak v praxi není příliš užitečné uvažovat.

2.2.1 Konstrukce MDS matic tvaru 4×4 pomocí minorů

Jak bylo dokázáno v Tvrzení 21, až na cyklický posun a přenásobení nenulovým prvkem tělesa $\mathbb{F}$, mohou existovat pouze dva typy cirkulantních MDS matic tvaru 4×4 nad tělesem $\mathbb{F}$ a to $\mathrm{Circ}(a, b, 1, 1)$ a $\mathrm{Circ}(1, a, b, c)$ pro nějaké po dvou různé nenulové prvky $a, b, c, 1$ tělesa $\mathbb{F}$.

Při konstrukci MDS matic můžeme podle Důsledku 7, podobně jako v předchozích sekcích, testovat (ne)nulovost minorů (tj. determinantů podmatic) a podle toho určit, zda se jedná o MDS matici, nebo ne. U cirkulantních MDS matic tvaru $d \times d$ je možné využít opakujících se minorů podmatic tvaru $(d-1) \times (d-1)$.

Lemma 24. *Buď M regulární matice tvaru $d \times d$ nad tělesem $\mathbb{F}$, potom M^{-1} tvaru $d \times d$ obsahuje pouze nenulové prvky (tj. prvky $\mathbb{F}^*$) právě tehdy, když je determinant každé podmatice tvaru $(d-1) \times (d-1)$ matice M nenulový.*

Důkaz: Matice M je regulární, existuje tedy M^{-1} a $\det(M) \neq 0$. Z lineární algebry [4, Věta 7.38] víme, že $M^{-1} = (\det(M))^{-1} \cdot \mathrm{Adj}(M)$, kde $\mathrm{Adj}(M)$ značí matici adjungovanou k matici M, tj. matici transponovanou k matici tvořené až na znaménko minory podmatic tvaru $(d-1) \times (d-1)$ matice M. Všechny prvky M^{-1} jsou tak nenulové právě tehdy, když jsou všechny minory podmatic tvaru $(d-1) \times (d-1)$ matice M nenulové.

□

Lemma 25. *Buď M cirkulantní MDS matice tvaru $d \times d$ nad konečným tělesem $\mathbb{F}_q$, potom je M^{-1} cirkulantní matice tvaru $d \times d$ obsahující pouze nenulové prvky.*

Důkaz: MDS matice M je regulární a stejně tak je regulární každá její podmatice. Matice M^{-1} tak existuje a podle Lemmatu 24 obsahuje pouze nenulové prvky. Dle Lemmatu 17 je inverzní matice k regulární cirkulantní matici nad konečným tělesem $\mathbb{F}_q$ cirkulantní matice stejného tvaru.

□

Poznámka. Lemma 25 platí dle poznámky za Lemmatem 17 rovněž pro nekonečné těleso $\mathbb{F}$.

Nyní se budeme snažit zkonstruovat cirkulantní MDS matici

$$M = \mathrm{Circ}(a, b, 1, 1) = \begin{pmatrix} a & b & 1 & 1 \\ 1 & a & b & 1 \\ 1 & 1 & a & b \\ b & 1 & 1 & a \end{pmatrix}$$

nad tělesem $\mathbb{F}$.

Dle Důsledku 7 můžeme postupovat tak, že budeme postupně volit prvky $a, b \in \mathbb{F}^* \backslash \{1\}, a \neq b$ a ověřovat, zda jsou minory všech jejích podmatic nenulové.

Pro samotnou matici M (tj. podmatici tvaru 4×4) tak dostáváme determinant rovný $a^4 - 2a^2 + 4a - b^4 + 4ab^2 + 2b^2 - 4a^2b - 4b$.

Pro podmatice tvaru 3×3 matice M můžeme dle Lemmatu 24 místo minorů ekvivalentně ověřovat, zda matice M^{-1} obsahuje pouze nenulové prvky. Podle Lemmatu 25 a poznámky za ním je matice M^{-1} navíc cirkulantní, stačí tedy ověřovat pouze 4 hodnoty.

Matici M^{-1} je možné získat buďto Gauss-Jordanovou eliminací nebo jako součin $(\det(M))^{-1} \cdot \mathrm{Adj}(M)$, kde $\mathrm{Adj}(M)$ je matice adjungovaná k matici M. $\mathrm{Adj}(M)$ není těžké spočítat, musí být stejně jako matice M^{-1} cirkulantní. Stačí určit determinanty podmatic tvaru 3×3 matice $\mathrm{Circ}(a, b, 1, 1)$ po vynechání prvního

řádku a dle definice adjungované matice je přenásobit $(-1)^j$, kde $j = 0, \ldots, 3$ je index sloupce.

Matice $\mathrm{Adj}(M)$ se tak rovná matici

$$\mathrm{Circ}(a^3-2ba-a+b^2+1, 2ab+b-b^3-a^2-1, b^2a-a^2+a-2b+1, 2a+b^2-ba^2-b-1)^T.$$

Tato matice je z Lemmatu 12 rovná matici

$$\mathrm{Circ}(a^3-2ba-a+b^2+1, 2a+b^2-ba^2-b-1, b^2a-a^2+a-2b+1, 2ab+b-b^3-a^2-1).$$

Potom platí až na znaménko následující rovnosti:

$$M^{-1} = (\det(M))^{-1} \cdot \mathrm{Adj}(M) = (a^4 - 2a^2 + 4a - b^4 + 4ab^2 + 2b^2 - 4a^2b - 4b)^{-1} \cdot$$

$$\cdot \mathrm{Circ}(a^3-2ba-a+b^2+1, 2a+b^2-ba^2-b-1, b^2a-a^2+a-2b+1, 2ab+b-b^3-a^2-1).$$

Protože jsme v tělese, součin dvou nenulových prvků je nenulový. Matice M^{-1} tak obsahuje pouze nenulové prvky právě tehdy, když jsou všechny výrazy

$$a^3 - 2ba - a + b^2 + 1, 2a + b^2 - ba^2 - b - 1, b^2a - a^2 + a - 2b + 1, 2ab + b - b^3 - a^2 - 1$$

nenulové.

Pokud označíme M' matici vzniklou z M vynecháním prvního řádku, jedná se až na znaménko o minory podmatic tvaru 3×3 matice M'. Inverzní matici tak není nutné počítat. Lemmata 24 a 25 však mají obecnou podobu, kdybychom tímto způsobem zkoumali MDS vlastnost větších cirkulantních matic, výpočet inverzní matice by se časově vyplatil.

Pro podmatice tvaru 2×2 již tento trik použít nemůžeme, protože podmatice tvaru 3×3 matice M obecně nejsou cirkulantní. Je tak nutné ověřit nenulovost všech minorů těchto podmatic.

Například pro podmatici

$$\begin{pmatrix} a & b & 1 \\ 1 & a & b \\ 1 & 1 & a \end{pmatrix}$$

dostáváme následující minory: $a^2 - b, a - b, 1 - a, ab - 1, a^2 - 1, b^2 - a$.

Odpověď na to, jaké minory podmatic tvaru 2×2 matice M obsahuje, nám dává následující lemma.

Lemma 26. *Pro cirkulantní matici* $M = \mathrm{Circ}(a, b, 1, 1)$ *nad tělesem* $\mathbb{F}$ *existují až na znaménko následující minory jejích podmatic tvaru* 2×2*:*

$$a - 1, b - 1, b - a, a^2 - 1, a^2 - b, ab - 1, b^2 - 1, b^2 - a.$$

Důkaz: Matice M obsahuje pouze prvky z množiny $\{1, a, b\}$. Rozepsáním všech součinů dvou prvků této množiny dostaneme posloupnost $(1, a, b, a^2, ab, b^2)$. Každý determinant podmatice 2×2 matice M je rozdílem dvou těchto součinů.

Na nulovost přitom nemá vliv jejich pořadí ($a - 1 \neq 0 \Leftrightarrow 1 - a \neq 0$), stačí tak uvažovat pouze prvky posloupnosti $(1, a, b, a^2, ab, b^2)$ na indexech i, j takových, že $i \leq j$.

Obecně můžou být některé prvky posloupnosti shodné. To by potom znamenalo, že některé minory budou splývat. Pro nalezení všech minorů, uvažujme tedy v průběhu důkazu, že posloupnost $(1, a, b, a^2, ab, b^2)$ obsahuje po dvou různé prvky.

Pro existenci minoru $1 - 1$ by matice M musela obsahovat podmatici

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Tuto podmatici však zřejmě neobsahuje.

Ze struktury matice M se prvky a, b nemohou vyskytovat v obou členech rozdílu zároveň (nemůžeme získat například determinant $a^2 - a$). To by totiž znamenalo, že matice M obsahuje v některém z řádků nebo sloupců některý z prvků a, b alespoň dvakrát. To však z cirkulantnosti matice a rozdílnosti a, b není možné.

Pro existenci minoru $a^2 - b^2$ až na znaménko by matice M musela obsahovat jednu z podmatic

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \begin{pmatrix} b & a \\ a & b \end{pmatrix}.$$

Ani jednu z těchto podmatic však zřejmě neobsahuje (M je cirkulantní matice tvaru většího než 2×2 a první řádek obsahuje prvky a, b v tomto pořadí bezprostředně za sebou).

Z dosavadní diskuse jsme (až na znaménko) vyloučili všechny možné minory podmatic tvaru 2×2 matice M kromě následujících:

$$a - 1, b - 1, b - a, a^2 - 1, a^2 - b, ab - 1, b^2 - 1, b^2 - a.$$

Dokážeme, že všechny zbylé minory matice M obsahuje. Je snadné nahlédnout, že

$$M = \begin{pmatrix} a & b & 1 & 1 \\ 1 & a & b & 1 \\ 1 & 1 & a & b \\ b & 1 & 1 & a \end{pmatrix}$$

obsahuje všechny následující podmatice tvaru 2×2:

$$\begin{pmatrix} a & b \\ 1 & a \end{pmatrix}, \begin{pmatrix} a & 1 \\ 1 & b \end{pmatrix}, \begin{pmatrix} a & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ b & 1 \end{pmatrix}, \begin{pmatrix} b & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} a & 1 \\ 1 & a \end{pmatrix}, \begin{pmatrix} b & 1 \\ 1 & b \end{pmatrix}$$

a matice M tak má až na znaménko následující minory:

$$a^2 - b, ab - 1, a - 1, a - b, a - b^2, b - 1, a^2 - 1, b^2 - 1.$$

□

Shrnutím dostáváme následující tvrzení.

Tvrzení 27. *Matice* $M = \mathrm{Circ}(a, b, 1, 1)$ *nad tělesem* $\mathbb{F}$ *je MDS právě tehdy, když* zároveň *z podmínek kladených na*

- *Matici* M *tvaru* 4×4 *platí:*

$$a^4 - 2a^2 + 4a - b^4 + 4ab^2 + 2b^2 - 4a^2b - 4b \neq 0,$$

- *Podmatice M tvaru 3×3 platí:*

$$a^3 - 2ba - a + b^2 + 1 \neq 0,$$

$$2a - ba^2 + b^2 - b - 1 \neq 0,$$

$$b^2a - a^2 + a - 2b + 1 \neq 0,$$

$$2ab - b^3 + b - a^2 - 1 \neq 0,$$

  (ekvivalentně M^{-1} obsahuje pouze nenulové prvky).

- *Podmatice M tvaru 2×2 platí: Výrazy*

$$a - 1, b - 1, b - a, a^2 - 1, a^2 - b, ab - 1, b^2 - 1, b^2 - a$$

  jsou nenulové.

- *Podmatice M tvaru 1×1 platí: Matice M obsahuje pouze nenulové prvky, ekvivalentně $a, b \neq 0$.*

Poznámka. Pro cirkulantní matici $M = \mathrm{Circ}(a, b, c, 1)$ můžeme podobně sestavit podmínky, za kterých je MDS, budou však mnohem složitější.

Podmínky z Tvrzení 27 můžeme dále zjednodušit, například pro konečné těleso charakteristiky dva dostáváme následující tvrzení.

Tvrzení 28. *Nechť $a, b, 1$ jsou po dvou různé nenulové prvky tělesa $\mathbb{F}_{2^n}$ takové, že a, b nejsou navzájem inverzní, přičemž b není obrazem ani vzorem prvku a při Frobeniově automorfismu tělesa $\mathbb{F}_{2^n}$ (tj. $a^2 \neq b, b^2 \neq a$). Potom existuje matice M^{-1} inverzní k matici $M = \mathrm{Circ}(a, b, 1, 1)$ a obsahuje-li M^{-1} pouze nenulové prvky, je matice M cirkulantní MDS matice.*

Důkaz: Matice M^{-1} inverzní k matici M existuje právě tehdy, když je M regulární, což nastane právě tehdy, když

$$\det(M) = a^4 - b^4 \neq 0 \Leftrightarrow (a - b)^4 \neq 0 \Leftrightarrow a \neq b.$$

Z předpokladu, že $a, b \in \mathbb{F}_{2^n}$ jsou různé, matice M^{-1} existuje. Ověříme, zda máme splněny všechny podmínky kladené na podmatice pro to, aby byla matice $M = \mathrm{Circ}(a, b, 1, 1)$ MDS.

- Prvky a, b jsou nenulové, podmínky kladené na podmatice tvaru 1×1 jsou proto splněny.

- Prvky a, b nejsou rovny 1, navíc jsou navzájem různé, $a^2 \neq 1$, protože $a \neq 1 = -1$, stejně tak $b^2 \neq 1$. Prvky a, b nejsou navzájem inverzní, tedy $ab \neq 1$. Prvek b není obrazem ani vzorem prvku a při Frobeniově automorfismu tělesa $\mathbb{F}_{2^n}$, tedy $a^2 \neq b$ a $b^2 \neq a$, a tak jsou všechny podmínky kladené na podmatice tvaru 2×2 splněny.

- Matice M^{-1} z předpokladu obsahuje pouze nenulové prvky, podmínky kladené na podmatice tvaru 3×3 jsou tudíž splněny.

- Matice M je regulární, podmínka kladená na (pod)matici M tvaru 4×4 je také splněna.

Matice M je tak podle Tvrzení 27 MDS.

□

Tímto způsobem je možné vybírat prvky $a, b \in \mathbb{F}_{2^n}^* \backslash \{1\}, a \neq b$ a ověřovat, zda jsou podmínky pro cirkulantní MDS matici $\mathrm{Circ}(a, b, 1, 1)$ splněny. O tom, že matice není MDS se dozvíme rychle a můžeme tak testovat další prvky tělesa. Potvrzení MDS vlastnosti matice trvá o něco déle.

2.3 Obecné MDS matice z Vandermondových matic

Z Důsledku 6 plyne následující lemma.

Lemma 29. *Čtvercová matice je MDS právě tehdy, když je každá její čtvercová podmatice MDS.*

Z Lemmatu 29 a již dříve uvedeného Lemmatu 8 bychom mohli uvažovat o blokové konstrukci cirkulantních MDS matic.

Příklad. Buď A bloková matice tvořená bloky B a C, kde B a C jsou cirkulantní MDS matice.

$$A = \begin{pmatrix} B & C \\ C & B \end{pmatrix}$$

Takto tvořit cirkulantní MDS matice však není možné. Označíme-li

$$B = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \text{ a } C = \begin{pmatrix} c & d \\ d & c \end{pmatrix},$$

kde a, b, c, d jsou prvky $\mathbb{F}^*$, potom z podmínky na cirkulantnost matice A dostáváme $b = d$ a matice tak dle Tvrzení 21 není biregulární, tedy ani MDS.

Obecnější matice však můžeme konstruovat z takzvaných Vandermondových matic. Tato část vychází z článku [7, str. 794-795].

Definice 9 (Vandermondova matice)**.** *Buď $\mathbb{F}$ těleso. Matice*

$$\mathrm{Vand}(a_0, a_1, \ldots, a_{n-1}) = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_0^2 & a_1^2 & a_2^2 & \ldots & a_{n-1}^2 \\ \vdots & \vdots & & \vdots & \\ a_0^{n-1} & a_1^{n-1} & a_2^{n-1} & \ldots & a_{n-1}^{n-1} \end{pmatrix},$$

kde $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}$, se nazývá Vandermondova matice.

Z lineární algebry víme, že determinant Vandermondovy matice

$$\det(\mathrm{Vand}(a_0, a_1, \ldots, a_{n-1})) = \prod_{0 \le j < i \le n-1} (a_j - a_i)$$

je nenulový právě tehdy, když $a_i \neq a_j$ kdykoli $i \neq j$.

Věta 30. [7, Theorem 4.2] *Nechť*

$$A = \mathrm{Vand}(a_0, a_1, \ldots, a_{n-1}) \text{ a } B = \mathrm{Vand}(b_0, b_1, \ldots, b_{n-1})$$

jsou dvě Vandermondovy matice takové, že prvky $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in \mathbb{F}$ *jsou po dvou různé. Potom jsou matice* $A^{-1}B$ *a* $B^{-1}A$ *MDS.*

Důkaz: Dokážeme, že $A^{-1}B$ je MDS matice. Pro $B^{-1}A$ je důkaz analogický. Označme $U = [A|B]$ matici tvaru $n \times 2n$ a uvažujme součin $W = A^{-1}U = [I_n|R]$, kde $R = A^{-1}B$. Dokážeme, že kód s generující maticí W je MDS. Každá $n \times n$ podmatice U je regulární, protože je to Vandermondova matice tvořená n-ticí různých prvků. U je potom dle Lemmatu 4 MDS kód. Matice A^{-1} je regulární, a tedy součinem elementárních matic, jejichž násobení zleva nemění řádkový prostor matice. Řádkové prostory matic U a W jsou tak stejné a generují stejný kód. Tedy W je rovněž MDS kód a $R = A^{-1}B$ je z definice MDS matice.

□

2.4 MDS matice vhodné pro kryptografii

Pro použití matic v kryptografii je vhodné, aby byla jejich implementace co nejjednodušší. Tím je možné předejít mnoha implementačním chybám. Při návrhu matic používaných v kryptogafii se tedy často požaduje, aby šlo o involuční nebo ortogonální matice. Involuční matice je čtvercová matice A taková, že $A^2 = I$, tedy $A^{-1} = A$. Dále se budeme věnovat ortogonálním maticím.

Definice 10 (Ortogonální matice)**.** *Čtvercová matice* A *se nazývá* ortogonální*, pokud platí* $AA^T = I$*, tedy* $A^{-1} = A^T$*.*

Při dešifrování se využívá inverzní matice A^{-1}. Pokud je matice A involuční nebo ortogonální, není nutné A^{-1} implementovat, stačí nám samotná matice A (resp. její transpozice). Požadavek na ortogonalitu je tak častý a opodstatněný, ovšem u cirkulantních matic tvaru $2^d \times 2^d$ nad tělesem $\mathbb{F}_{2^n}$ jej není možné splnit.

Tvrzení 31. [1, Lemma 5] *Neexistuje žádná ortogonální cirkulantní MDS matice tvaru* $2^d \times 2^d$ *nad tělesem* $\mathbb{F}_{2^n}$*.*

Důkaz: Předpokládejme, že $A = \mathrm{Circ}(a_0, a_1, \ldots, a_{2^d-1})$ je ortogonální cirkulantní matice, kde $a_0, a_1, \ldots, a_{2^d-1} \in \mathbb{F}_{2^n}$ dokážeme, že není MDS.

Označme R_i, pro $i = 0, \ldots, 2^d - 1$, i-tý řádkový vektor matice A, potom $R_i = (a_{0-i}, a_{1-i}, \ldots, a_{2^d-1-i})$ s indexy počítanými modulo 2^d. Protože předpokládáme, že matice A je ortogonální, musí být bodový součin $R_i \cdot R_j$ pro $i \neq j$ roven nule, speciálně $R_0 \cdot R_j = 0$ pro $j \in \{2k+1; k = 0, 1, \ldots, 2^{d-2} - 1\}$.

Jedná se o součin

$$R_0 \cdot R_j = (a_0, a_1, \ldots, a_{2^d-1}) \cdot (a_{0-j}, a_{1-j}, \ldots, a_{2^d-1-j}) = \sum_{i=0}^{2^d-1} a_i a_{i-j} = \sum_{k=0}^{2^d-1} a_{k+j} a_k.$$

Z toho plynou následující rovnice

$$\sum_{i=0}^{2^d-1} a_i a_{i+1} = 0, \sum_{i=0}^{2^d-1} a_i a_{i+3} = 0, \sum_{i=0}^{2^d-1} a_i a_{i+5} = 0, \ldots, \sum_{i=0}^{2^d-1} a_i a_{i+2^{d-1}-1} = 0$$

s indexy počítanými modulo 2^d.

V každé z předchozích rovnic se zřejmě násobí vždy prvky s indexy opačných parit. Navíc se každý prvek a_i, kde $i = 0, \ldots, 2^d - 1$, vyskytuje v každé rovnici právě dvakrát a v rovnici $\sum_{i=0}^{2^d-1} a_i a_{i+2k+1}$ je vynásoben prvky $a_{i+2k+1}, a_{i-(2k+1)}$ pro všechna $k = 0, 1, \ldots 2^{d-2} - 1$. Tedy v součtu všech 2^{d-2} rovnic se a_i vyskytuje dohromady 2^{d-1}-krát a je vynásobeno všemi prvky s indexy opačné parity. Prvků s indexy opačné parity je přesně 2^{d-1}, tedy a_i je vynásobeno všemi prvky opačné parity právě jednou. Dostáváme tak rovnici

$$(a_0 + a_2 + \cdots + a_{2^d-2})(a_1 + a_3 + \cdots + a_{2^d-1}) = 0,$$

kde je alespoň jeden z uvedených činitelů roven 0.

Matice A obsahuje podmatici $\mathrm{Circ}(a_0, a_2, \ldots, a_{2^d-2})$ vzniklou výběrem řádků a sloupců na sudých pozicích a podmatici $\mathrm{Circ}(a_1, a_3, \ldots, a_{2^d-1})$ vzniklou výběrem řádků na sudých a sloupců na lichých pozicích. Obě jsou tvaru $2^{d-1} \times 2^{d-1}$.

Podle Tvrzení 19 platí

$$\det(\mathrm{Circ}(a_0, a_2, \ldots, a_{2^d-2})) = \sum_{i=0}^{2^{d-1}-1} a_{2i}^{2^{d-1}} = (a_0 + a_2 + \cdots + a_{2^d-2})^{2^{d-1}}$$

obdobně

$$\det(\mathrm{Circ}(a_1, a_3, \ldots, a_{2^d-1})) = \sum_{i=0}^{2^{d-1}-1} a_{2i+1}^{2^{d-1}} = (a_1 + a_3 + \cdots + a_{2^d-1})^{2^{d-1}}.$$

V posledních rovnostech využíváme toho, že jsme v tělese charakteristiky 2 a mocnění na druhou, tedy také mocnění na 2^{d-1}, je potom homomorfismus.

Determinant alespoň jedné z těchto dvou podmatic je tedy roven 0 a matice A tak není MDS.

□

Příklad. Mějme cirkulantní matici $A = \mathrm{Circ}(a_0, a_1, a_2, a_3)$, kde $a_0, a_1, a_2, a_3 \in \mathbb{F}_{2^n}$ a předpokládejme, že A je ortogonální, potom $R_0 = (a_0, a_1, a_2, a_3)$, a tedy pro $j \in \{2k + 1; k = 0, 1, \ldots, 2^{2-2} - 1\} = \{1\}$ dostáváme

$$R_0 \cdot R_1 = (a_0, a_1, a_2, a_3) \cdot (a_3, a_0, a_1, a_2).$$

Dostaneme tak jediný součet $\sum_{i=0}^{2^2-1} a_i a_{i+1} = 0$ a z něho rovnici

$$a_0 a_1 + a_1 a_2 + a_2 a_3 + a_3 a_0 = (a_0 + a_2)(a_1 + a_3) = 0.$$

Matice

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ a_3 & a_0 & a_1 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_1 & a_2 & a_3 & a_0 \end{pmatrix}$$

obsahuje podmatice

$$\mathrm{Circ}(a_0, a_2) = \begin{pmatrix} a_0 & a_2 \\ a_2 & a_0 \end{pmatrix} \text{ a } \mathrm{Circ}(a_1, a_3) = \begin{pmatrix} a_1 & a_3 \\ a_3 & a_1 \end{pmatrix}$$

tvaru $2^{2-1} \times 2^{2-1}$.

Jejich determinant je podle Tvrzení 19 roven

$$a_0^{2^{2-1}} + a_2^{2^{2-1}} = (a_0 + a_2)^2 = a_0 + a_2 \text{ resp. } a_1^{2^{2-1}} + a_3^{2^{2-1}} = (a_1 + a_3)^2 = a_1 + a_3$$

a alespoň jeden z těchto výrazů je roven 0.

3. Využití MDS matic

Tato kapitola se stručně zabývá využitím MDS matic v kryptografii. Koncepty používané v kryptografii však není možné shrnout do krátké kapitoly, jde tak spíše o nástin, ne o detailní popis.

MDS matice v kryptografii nachází využití především v blokových šifrách. Slouží jako difúzní vrstva, která má za úkol rozprostřít charakteristiky otevřeného textu do co největší části textu šifrového. Díky této vrstvě se při nepatrné změně otevřeného textu změní šifrový text významným způsobem, útočníkovi tak ztěžuje například rozpoznání dvojice podobných zpráv nebo třeba použití lineární a diferenciální kryptoanalýzy.

Tvrzení 32. *Matice*

$$A = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}$$

zapsaná v šestnáctkové soustavě používaná v AES [1] *je cirkulantní MDS matice nad tělesem* $\mathbb{F}_{2^8}$.

Uvažujme irreducibilní polynom

$$\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1 \in \mathbb{F}_2[\alpha]$$

stupně osm. Prvky tělesa $\mathbb{F}_{2^8}$ pak můžeme reprezentovat jako polynomy ležící v $\mathbb{F}_2[\alpha]/(\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1)$. Jeho prvky je tak možné reprezentovat jako dvouciferná čísla v šestnáctkové (hexadecimální) soustavě a to následujícím způsobem: prvek $a_7\alpha^7 + a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 \in \mathbb{F}_{2^8}$ obsahuje právě osm koeficientů $\mathbb{F}_2$. Tuto posloupnost můžeme též chápat jako binární zápis čísla $(a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1\ a_0)_2$, které můžeme následně reprezentovat v šestnáctkové soustavě. Prvek 02 tak odpovídá prvku α, prvek 03 odpovídá prvku $\alpha + 1$ a tak dále.

V předchozí kapitole, konkrétně v Tvrzení 23, jsme ukázali, že je výše uvedená matice MDS. Všimněme si, že se jedná o matici s velkým množstvím jedniček a dvojek. To není náhoda, šifrování pomocí matic s malými prvky je rychlé, protože násobení jedničkou je identita a násobení dvěma v binární soustavě znamená pouze posun v bitovém zápisu o jednu pozici vlevo.

Uvažujme nyní zobrazení pomocí MDS matice A tvaru $m \times m$. Změna jedné složky vstupního vektoru má za následek změnu všech složek vektoru výstupního. Obecně pak změna t složek vstupu zapříčiní změnu alespoň $m - t + 1$ složek výstupu. Použití lineární transformace založené na MDS maticích jako vrstvy kola iterované blokové šifry (např. MixColumns v algoritmu AES[1]) tak výrazným způsobem komplikuje její lineární a diferenciální kryptoanalýzu[2]. Pro konstrukci kvalitních lineárních a diferenciálních cest[3] využívaných v kryptografických útocích je důležité omezení počtu takzvaných aktivních S-Boxů[4]. Změny v počtu

nenulových složek vektorů při transformaci MDS maticemi takovéto konstrukce pro větší počet kol prakticky znemožňují[5].

Následující poznámky si kladou za cíl přiblížit kryptografické pojmy lidem, kteří se kryptografií přímo nezabývají. Nejedná se tak o přesné vysvětlení principů, jde spíše o stručný nástin srozumitelný širší skupině lidí.

Poznámka (1). Bloková šifra AES byla navržena jako rozšíření tzv. Substitučně permutační síťe. Skládá se z určitého počtu kol, kde každé kolo obsahuje záměnu bajtů (SubBytes) pomocí S-Boxů[4], posunutí řádků (ShiftRows), promíchání sloupců (MixColumns) pomocí MDS matice uvedené v Tvrzení 32 a přidání kolových klíčů (AddRoundKey).

Poznámka (2). Lineární kryptoanalýza je útok založený na zkoumání pravděpodobnosti lineární kombinace vstupních a výstupních bitů. Diferenciální kryptoanalýza je založená na zkoumání pravděpodobnosti diference výstupních bitů při dané diferenci vstupních bitů. Na základě spočítaných pravděpodobností (tj. korelační matice S-Boxu při lineární kryptoanalýze nebo matice šíření diference S-Boxu při diferenciální kryptoanalýze) se pak útočník snaží konstruovat lineární nebo diferenciální cesty[3]. Po získání dostatečného množství vzorků dvojic [otevřený text, šifrový text] tipuje část posledního kolového klíče a pokud reálná pravděpodobnost odpovídá spočítané, získal pravděpodobně část posledního kolového klíče.

Poznámka (3). Lineární a diferenciální cesty popisují možný průběh šifrování zprávy. Jedná se o posloupnosti binárních vektorů (resp. jejich diferenci) vystupující v jednotlivých kolech šifry. Při útoku jsou používány cesty s co možná největší (případně nejmenší) pravděpodobností a malým počtem výstupních bitů (resp. malou diferencí binárních vektorů). Vysoká pravděpodobnost umožňuje redukovat počet nutných vzorků, malý počet bitů usnadňuje hledání cesty s malým počtem aktivních S-Boxů.

Poznámka (4). S-Box je bijektivní tabulka hodnot vstupů a výstupů určitých rozměrů. V blokové šifře zajišťuje nelineární substituci. Při průchodu S-Boxem dávají stejné vstupy pochopitelně stejný výstup, těmto S-Boxům se říká pasivní. Různé vstupy naopak dávají různé výstupy, takovým S-Boxům se říká aktivní. Pokud je velké množství S-Boxů aktivních, dochází k substituci velké části vstupu a tím pádem výraznému vlivu kolového klíče na výstupní text.

Poznámka (5). V šifře AES se pomocí MDS matice (operace MixColumns) jeden nenulový bajt promění ve čtyři nenulové bajty. Ve druhém kole se pomocí kombinace operací ShiftRows a MixColumns nenulovost rozšíří do všech šestnácti bajtů, čímž aktivuje S-Box na všech částech šifry.

Na druhou stranu kombinace ShiftRows a MixColumns umožňuje některé útoky na AES jako například impossible differentials, tj. vyloučení těch klíčů, které mají pro dva různé otevřené texty diferenci, jež nemůže nastat.

Podrobněji se významem této matice v AES zabývá kniha [8], především kapitola The Wide Trail Design Strategy. O útocích pomocí impossible differentials je možné se dočíst v článku [9].

Závěr

Cílem práce bylo popsat konstrukci MDS matic. Práce se zabývala především cirkulantními MDS maticemi převážně nad konečnými tělesy. Potřebovali jsme vybudovat matematický aparát propojující oblasti samoopravných kódů, lineární i obecné algebry a konečných těles. Tento matematický aparát zahrnoval důležitou charakterizaci MDS matic pomocí determinantů jejich podmatic a zavedení pojmu cirkulantní matice tvaru $d \times d$. Dokázali jsme, že tyto matice tvoří komutativní algebru nad tělesem, jež je izomorfní faktorové algebře polynomů stupně nejvýše $d - 1$. V další sekci jsme zadefinovali biregulární matice, vysvětlili jejich vztah k MDS maticím a uvedli, jaké vlastnosti musí splňovat prvky cirkulantní biregulární MDS matice tvaru 4×4. To nám dalo omezující podmínky na strukturu cirkulantních MDS matic tohoto tvaru, protože každá MDS matice musí být biregulární. Dozvěděli jsme se tak, že existují pouze dva typy cirkulantních MDS matic tohoto tvaru, totiž $\mathrm{Circ}(a, b, 1, 1)$ a $\mathrm{Circ}(a, b, c, 1)$. V následující kapitole jsme již konstruovali samotné MDS matice. Nejdříve šlo o cirkulantní MDS matice tvarů 3×3 a 4×4 nad konečným tělesem charakteristiky dva, poté o cirkulantní MDS matice tvaru 4×4 nad obecným tělesem, jež byly konstruovány pomocí minorů. Kapitola obsahovala také konstrukci obecných MDS matic pomocí Vandermondových matic. V závěru kapitoly jsme uvedli, že neexistuje žádná ortogonální cirkulantní MDS matice tvaru $2^d \times 2^d$ nad tělesem charakteristiky dva. Poslední kapitola se krátce zmiňovala o použití MDS matic v kryptografii.

Přínos této práce spočívá především ve vlastním přístupu ke konstrukci cirkulantních MDS matic tvaru 4×4 typu $\mathrm{Circ}(a, b, 1, 1)$ pomocí minorů, tedy sekci 2.2.1. To se povedlo za pomoci Tvrzení 21 a Důsledku 7. Bylo třeba formulovat a dokázat Lemmata 24, 25 a 26, ze kterých plynou Tvrzení 27 a 28. Ta dávají relativně kompaktní charakterizaci MDS cirkulantních matic tvaru 4×4 typu $\mathrm{Circ}(a, b, 1, 1)$. Pomocí této, pro konečná tělesa celkem snadno ověřitelné, charakterizace je možné poměrně jednoduše ověřit, zda je daná cirkulantní matice MDS, a postupným dosazováním prvků nějakou cirkulantní MDS matici zkonstruovat.

Další přínos práce vidím v doplnění důkazů, které byly v původních článcích méně podrobné, nebo nebyly uvedeny vůbec (např. 11, 12, 13, 18, 21, 23). Vlastní přínos lze spatřit také ve formulaci některých dalších tvrzení a předvedení jejich důkazů (např. 10, 15, 16, 20) nebo v předložení vlastních příkladů a poznámek, které čtenáři pomáhají pochopit uvedená tvrzení či jejich důkazy.

Při psaní této bakalářské práce jsem se pokoušel konstruovat MDS matice pomocí Reed-Solomonových kódů, k dostatečně zajímavým závěrům jsem však nestihl dojít. Jistě by bylo zajímavé se ke zkoumání takové konstrukce vrátit. Práci by také bylo možné rozšířit o podmínky kladené na cirkulantní MDS matice tak, aby obsahovaly co nejvíce jedniček a byly involuční nebo ortogonální, a tedy vhodné pro kryptografii. Dále by bylo zajímavé zkoumat tyto podmínky pro MDS matice tvořené z Vandermondových matic. A v neposlední řadě by bylo přínosné matematicky rozvést poslední kapitolu o tom, jakou roli MDS matice v kryptografii zastávají, případně jak se tato role změní s příchodem nových technologií (například kvantových počítačů).

Seznam použité literatury

[1] Kishan Chand Gupta and Indranil Ghosh Ray. Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. *Cryptogr. Commun.*, 7(2):257–287, 2015.

[2] Aleš Drápal. Samoopravné kódy. `https://manualzz.com/doc/15557095/skripta-a.-drápala-`. Naposledy navštíveno 30.12.2020.

[3] Tomáš Kaiser. Samoopravné kódy. `http://home.zcu.cz/~kaisert/kody/kody.pdf`. Naposledy navštíveno 30.12.2020.

[4] Libor Barto a Jiří Tůma. Lineární algebra. `https://www2.karlin.mff.cuni.cz/~barto/LinAlg/skripta_la5.pdf`. Naposledy navštíveno 30.12.2020.

[5] Libor Barto a Jiří Tůma. Konečná tělesa. `http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf`. Naposledy navštíveno 30.12.2020.

[6] Meicheng Liu and Siang Meng Sim. Lightweight MDS Generalized Circulant Matrices. *IACR Cryptol. ePrint Arch.*, 2016:186, 2016.

[7] Kishan Chand Gupta, Sumit Kumar Pandey, Indranil Ghosh Ray, and Susanta Samanta. Cryptographically significant MDS matrices over finite fields: A brief survey and some generalized results. *Adv. Math. Commun.*, 13(4):779–843, 2019.

[8] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[9] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New Impossible Differential Attacks on AES. 5365:279–293, 2008.