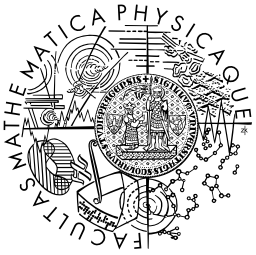


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁRSKA PRÁCA

Marek Bajtoš

Rýchle násobenie v telese GF(2^n)

Katedra algebry

Vedúci bakalárskej práce:	doc. Mgr. et Mgr. Žemlička Jan, Ph.D.
Študijný program:	Matematika
Študijný odbor:	Matematické metody informační bezpečnosti

Praha 2018

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

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 ..... dne ..... Podpis autora

Chcel by som poďakovať vedúcemu mojej bakalárskej práce doc. Mgr. et Mgr. Jánovi Žemličkovi Ph.D. za všetky cenné rady a pomoc pri písaní práce.

Názov práce: Rýchle násobenie v telese GF(2^n)

Autor: Marek Bajtoš

Katedra: Katedra algebry

Vedúci bakalárskej práce: doc. Mgr. et Mgr. Žemlička Jan, Ph.D., Katedra algebry

Abstrakt: V tejto bakalárskej práci budeme skúmať, ako optimalizovať násobenie fixným prvkom konečného telesa, ktoré je využiteľné pri implementácií šifrovacích algoritmov v ľahkej kryptografii. Efektívnosť násobenia budeme vyjadrovať pomocou počtu XOR operácií potrebných na implementáciu matice, ktorá reprezentuje daný fixný prvok konečného telesa. Dokážeme, že matica reprezentuje násobenie nejakým prvkom konečného telesa práve vtedy, keď je jej minimálny polynóm ireducibilný. Ďalej dokážeme tvrdenia, ktoré popisujú, za akých podmienok sa dá matica implementovať s 1 alebo 2 XOR operáciami. V závere práce uvedieme konštrukciu cyklických MDS matíc, v ktorých sa uplatní znalosť voľby prvkov konečného telesa, ktoré sa dajú ľahko implementovať.

Kľúčové slová: ľahká kryptografia, konečné teleso, XOR, MDS matica

Title: Fast multiplication in the field GF(2^n)

Author: Marek Bajtoš

Department: Department of Algebra

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

Abstract: In this bachelor thesis we research how to optimize multiplication with a fixed element of finite field which can be useful for implementation of cryptographic algorithms in lightweight cryptography. We will represent effectivity of multiplication by number of XOR operation needed for implementation of matrix which represent some fixed element of finite field. We prove that some matrix represents multiplication with some element of finite field if and only if the minimal polynomial of matrix is irreducible. We also prove theorems describing conditions which matrix must satisfy so matrix can be implemented with only 1 or 2 XOR operations. At the end of the thesis we show construction of circulant MDS matrices which uses elements of finite field with low XOR count so they can be easily implemented.

Keywords: lightweight cryptography, finite field, XOR, MDS matrix

Obsah

Úvod

V posledných rokoch sú na kryptografiu kladené neustále náročnejšie požiadavky. Jedným z problémov, s ktorými museli kryptografovia bojovať, je schopnosť bezpečnej komunikácie na zariadeniach, pre ktoré sú klasické kryptografické algoritmy príliš veľké, príliš pomalé alebo energeticky náročné. Tomuto odvetviu kryptografie sa dnes hovorí Ľahká kryptografia (Lightweight Cryptography). Hlavným cieľom ľahkej kryptografie je optimalizovať implementačné nároky šifrovania na zariadeniach s obmedzenou kapacitou, ale pritom neznížiť bezpečnosť šifrovania. Viac o tejto téme sa čitateľ môže dočítať napríklad v článku CryptoLUX (2016) alebo Mouha (2015).

Ako pekný príklad praktického použitia ľahkej kryptografie sa uvádzajú RFID (Radio-frequency identification) systémy, čo sú vlastne mikročipy, ktoré pomocou rádiovej komunikácie umožňujú sledovať napríklad polohu objednávky tovaru, športovca počas pretekov, knihy vypožičanej z knižnice alebo akéhokoľvek iného predmetu, ktorý tento čip má. Rovnaký princíp využívajú aj tzv. „chytré karty“, medzi ktoré môžeme zaradiť bezkontaktné karty, rôzne karty na vstup do budovy a iné. Samozrejme, na to, aby tento čip mohol bezpečne komunikovať s prijímačom, je potrebné komunikáciu šifrovať. Čip má veľmi malé rozmery a preto sa nám hodí ľahká kryptografia. Veľkosti čipov sa môžu pohyhovať rádovo v desatinách milimetrov. Podľa článku Swedberg (2017) vedci zo Stanford University pracujú na vývoji RFID čipu tak malého, že sa vojde do bunky ľudského tela. Doteraz najmenší čip využívajúci RFID technológiu bol vytvorený firmou Hitachi v roku 2003 a má veľkosť približne $0{,}3mm^2$, čo je asi veľkosť zrnka prachu, aj preto sa tento čip prezýva „powder“ alebo „dust“. Viac o čipe od spoločnosti Hitachi sa dá dočítať v článku Journal (2003) a o RFID sa dá dočítať v Cole a Ranasinghe (2008).

V dnešnej dobe sa v kryptografii pracuje prevažne s blokovými šiframi a hašovacími funkciami, a pre ich efektívnu implementáciu sa používajú substistučno-permutačné siete. Medzi blokové šifry, ktoré využívajú substitučno-permutačné siete a sú používané v ľahkej kryptografii, patria napríklad AES, LED a Midori (všetky 3 využívajú vo svojich schémach aj MDS matice, ktoré v závere uvedieme ako príklad využitia rýchleho násobenia v konečnom telese). Ako príklad hašovacej funkcie uveďme Merkle-Damgårdovu hašovaciu funkciu a PHOTON. Podrobnejší popis šifrovacích algoritmov ľahkej kryptografie a viac ich príkladov je uvedených v CryptoLUX (2016).

Ako teda ušetriť náklady na implementáciu kryptografických algoritmov pre zariadenia s obmedzenou kapacitou?

Konečné telesá hrajú v kryptografii dôležitú rolu, pretože veľa kryptografických schém ich využíva ako svoju základnú matematickú štruktúru. Z toho dôvodu si môžeme klásť otázku, či by sme vhodnou voľbou báze konečného telesa nemohli znížiť nároky na implementáciu daného šifrovacieho algoritmu. Odpoveďou na túto otázku je áno. Vhodná voľba báze v tomto zmysle navyše nemá vplyv na bezpečnosť danej schémy, ale môže značne znížiť náklady na implementáciu. V šifrách, ktoré sú založené na šifrovaní v kolách (rundách), je voľba vhodnej báze ešte o to výraznejšia, najmä pri násobení prvkom konečného telesa. V tejto práci sa preto pozrieme na to, ako takúto vhodnú reprezentáciu telesa voliť a ako zvoliť

reprezentáciu, ktorá bude optimálna pri násobení prvkom konečného telesa. Tejto problematike sme venovali kapitolu Efektívne násobenie v konečnom telese.

Ďalšiu možnosť zlepšenia efektivity implementácie v ľahkej kryptografii ponúka nami študovaný text Beierle a kol. (2016) vo vhodnej voľbe konštrukcie MDS matíc. Ako už bolo spomenuté, MDS matice využíva napríklad šifra AES. Tá využíva MDS maticu na reprezentáciu operácie mixovania stĺpcov (MixColumns), ktorá má zabezpečiť difúziu (čo je vlastnosť šifrovacieho algoritmu rozšíriť štatistické charakteristiky otvoreného textu na väčší úsek šifrového textu). Preto v závere práce stručne uvedieme konkrétnu konštrukciu MDS matíc, ktorých implementácia bude efektívna.

Spojením vhodnej reprezentácie konečného telesa a uvedenej konštrukcie MDS matíc (a to tak, že prvky matice volíme ako tie prvky konečného telesa, ktoré sa dajú efektívne implementovať) získame najefektívnejší spôsob implementácie MDS matíc, aký bol doteraz v literatúre predstavený. V našej práci sa ukazuje, ako pochopenie voľby reprezentácie telesa pozitívne ovplivní efektivitu implementácie.

Úvahy a možnosti vytvorenia efektívnejších algoritmov v ľahkej kryptografií pomocou vhodnej voľby reprezentácie konečného telesa a špeciálnej konštrukcie MDS matíc sme čerpali z článku Beierle a kol. (2016). Dôkazy dôležitých tvrdení doplníme o podrobnejšie vysvetlenie, pridáme znenia a niektoré dôkazy tvrdení, ktoré sú potrebné na dôkaz zaujímavých tvrdení uvedených v danom článku. Pripomenieme pojmy z konečných telies, lineárnej algebry a niektoré vlastnosti matíc, ktoré súvisia s danou problematikou a samotný článok viac priblížime čitateľovi, ktorý nie je v danej problematike zbehlý.

1. Základné pojmy a definície

V úvodnej kapitole uvedieme definíciu a popis matematických objektov, ktoré potrebujeme k porozumeniu problematiky ľahkého násobenia v telese. Pozrieme sa na polynomiálnu reprezentáciu konečných telies a na to, ako reprezentovať konečné teleso maticou. Nakoniec definujeme pojem počtu XOR operácií a jeho význam pre ďalšiu časť práce. Pripomenieme si aj základné vlastnosti daných objektov a uvedieme tvrdenia, ktoré budeme ďalej potrebovať.

1.1 Konečné telesá a ich polynomiálna reprezentácia

Na začiatok predstavíme značenie používané pre konečné telesá a popíšeme akú reprezentáciu konečných telies budeme uvažovať v ďalšej časti práce.

Chceme pracovať s konkrétnou reprezentáciou telesa s 2^n prvkami pre nejaké prirodzené n. Nasledujúca veta nám priblíži reprezentáciu prvkov konečného telesa, s ktorou budeme pracovať.

Veta 1.1. (O existencií rozšírenia telesa $\mathbb{F}$ určeného ireducibilným polynómom) *Nech $f(x) \in \mathbb{F}[x]$ je ireducibilný polynóm stupňa $n \in \mathbb{N}$ nad telesom $\mathbb{F}$. Potom faktorokruh $\mathbb{F}[x]/(f(x))$ je teleso obsahujúce $\mathbb{F}$ ako podteleso. Označme $\alpha = x + (f(x))$, potom α je koreňom $f(x)$ a $\mathbb{F}[\alpha] = \mathbb{F}[x]/(f(x))$ je rozkladové nadteleso polynómu f. Bázou tohto nadtelesa ako vektorového priestoru nad telesom $\mathbb{F}$ je $(\alpha^0, \ldots, \alpha^{n-1})$.*

Dôkaz. Veta plynie z tvrdení v práci Dummit a Foote (2004, Proposition 15., str. 313, Theorem 3. a Theorem 4., str. 512 - 513).

□

Poznamenajme, že v telese $\mathbb{F}[\alpha]$ sa počíta modulo polynóm $f(\alpha)$.

Keďže nebudeme pracovať s polynómami nad telesom $\mathbb{F}[\alpha]/(f(\alpha))$, ale zaujímajú nás len prvky tohto telesa reprezentované pomocou polynómov, budeme na miesto $f(\alpha)$ používať $f(x)$. To môžeme urobiť, pretože nás nezaujíma konkrétny koreň α polynómu $f(x)$, ale len reprezentácia telesa $\mathbb{F}[\alpha]/(f(\alpha))$ a tá je nezávislá na voľbe α ako koreňa polynómu $f(x)$, pretože teleso $\mathbb{F}[\alpha]/(f(\alpha))$ nie je jednoznačne určené.

Príklad 1.2. *Ak budeme uvažovať napríklad ireducibilný polynóm $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$, tak množina $\mathbb{F}_2[x]/(x^3+x+1)$ všetkých polynómov stupňa menšieho alebo rovného 2 s koeficientami v $\mathbb{F}_2$ a s operáciami sčítania a násobenia modulo $f(x)$ je podľa vety 1.1 teleso. Toto teleso obsahuje práve prvky*

$$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1.$$

Veta 1.3. (O existencií a jednoznačnosti konečných telies) *Každé konečné teleso má p^n prvkov, pre p prvočíslo a n prirodzené číslo.*

Pre každé prvočíslo p a prirodzené číslo n existuje teleso s p^n prvkami.

Ľubovoľné dve telesá s p^n prvkami sú izomorfné.

Dôkaz. Dôkaz je popísaný v práci Barto a Tůma (2017, str. 11). □

Teleso $\mathbb{F}_2[x]/(x^3+x+1)$ z príkladu 1.2 obsahuje práve 8 prvkov. Dá sa teda povedať, že toto teleso je podľa predchádzajúcej vety „rovnaké až na pomenovanie prvkov“ so všetkými telesami s 2^3 prvkami.

Na záver tejto sekcie uveďme štandardné značenie pre teleso s p^n prvkami.

Značenie 1.4. *Nech p je prvočíslo. Konečné teleso s p prvkami budeme označovať $\mathbb{F}_p$. Rozšírenie tohto telesa s p^n prvkami budeme označovať $\mathbb{F}_{p^n}$, pre nejaké $n \in \mathbb{N}$. Multiplikatívnu grupu telesa $\mathbb{F}$ budeme označovať $\mathbb{F}^*$.*

V našej práci budeme pracovať výhradne s binárnymi telesami a teda, podľa predchádzajúceho značenia, budeme pracovať s telesami $\mathbb{F}_{2^n} \cong \mathbb{F}_2[x]/(q(x))$, kde $q(x)$ je ireducibilný polynóm stupňa n.

1.2 Maticová reprezentácia konečných telies

Nasleduje predstavenie pojmov a definícií pre prácu s maticami nad konečným telesom. Pripomenieme, ako matica určuje lineárny operátor nad daným telesom, zavedieme značenie pre špeciálne typy matíc, pripomenieme pojmy minimálneho a charakteristického polynómu matice, zavedieme pojem doprovodnej matice polynómu a racionálnej kanonickej formy. Uvedieme niekoľko vlastností daných objektov, s ktorými budeme ďalej pracovať.

Značenie 1.5. (Okruh matíc nad telesom) *Okruh štvorcových matíc stupňa n nad telesom $\mathbb{F}$ budeme značiť $Mat_n(\mathbb{F})$, pre $n \in \mathbb{N}$.*

V nasledujúcom značení uvedieme niekoľko špeciálnych typov matíc v okruhu $Mat_n(\mathbb{F}_2)$ a spôsob ich označenia v našej práci.

Značenie 1.6. *Pre špeciálne matice stupňa n z okruhu $Mat_n(\mathbb{F}_2)$ budeme používať nasledujúce označenie:*

- *Pod symbolom $\mathbf{0}_n$ budeme rozumieť **nulovú maticu**.*
- *Pod symbolom I_n budeme rozumieť **jednotkovú maticu**.*
- *Matica $E_{i,j}$ bude matica, ktorá obsahuje samé nuly až na jednotku v i-tom riadku a v j-tom stĺpci, pre $i, j \in \{1,\ldots,n\}$.*
- ***Blokovo diagonálnu maticu** s d blokmi A_k, $k \in \{1,\ldots,d\}$ budeme značiť $\bigoplus_{k=1}^{d} A_k$.*

Značenie 1.7. *Ďalej budeme používať značenie:*

- *$wt(A)$ pre počet nenulových prvkov matice A.*
- *$wt(q)$ pre počet nenulových koeficientov polynómu q.*

Pripomeňme ešte, že prvky konečného telesa s charakteristikou p (v našom prípade s charakteristikou 2) sa dajú reprezentovať ako vektory s koeficientami v $\mathbb{F}_p$ ($\mathbb{F}_2$) vzhľadom na nejakú bázu telesa $\mathbb{F}_p$. Preto zavedieme označenie pre priradenie súradníc vzhľadom k danej báze.

Značenie 1.8. *Symbolom Φ_B budeme označovať bijektívne zobrazenie, ktoré priradzuje prvku $\alpha \in \mathbb{F}$ jeho súradnice vzhľadom k báze B telesa $\mathbb{F}$, resp. Φ_B^{-1} opačne.*

Pripomeňme reprezentáciu lineárneho operátoru pomocou matice.

Definícia 1.9. (Matica lineárneho operátoru) *Nech V je konečne dimenzionálny vektorový priestor nad telesom $\mathbb{F}$. Majme $f : V \to V$ lineárny operátor a $B = (v_1, v_2, \ldots, v_n)$ bázu priestoru V.* Maticu lineárneho operátoru f *vzhľadom k báze B rozumieme maticu*

$$A_B = (\Phi_B(f(v_1)), \Phi_B(f(v_2)), \ldots, \Phi_B(f(v_n))) \in Mat_n(K).$$

Veta 1.10. (Lineárny operátor pomocou matice) *Nech V je n-dimenzionálny vektorový priestor nad telesom $\mathbb{F}$. Každý lineárny operátor $f : V \to V$ sa dá popísať ako $\Phi_B(f(v)) = A_B\Phi_B(v)$ (násobenie maticou $A_B \in Mat_n(K)$ (z ľava)), kde B je ľubovoľná báza vektorového priestoru V.*

Dôkaz. Dôkaz tvrdenia sa dá nájsť v práci Barto a Tůma (2014, Tvrdenie 6.6, str. 197).

□

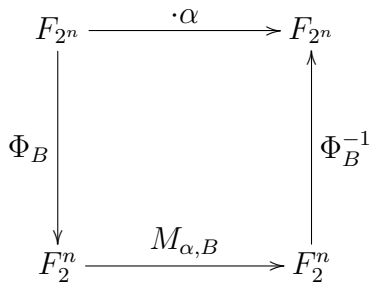
Všimnime si, že reprezentácia lineárneho operátoru je závislá na voľbe bázy B vektorového priestoru V (platí, že matica lineárneho operátoru je vzhľadom k jednej konkrétnej báze jednoznačná (to nebudeme dokazovať)). To znamená, že zmenou báze z B na B' sa zmení aj maticová reprezentácia lineárneho operátoru f. Túto transformáciu označujeme *zmena bázy*. Prechod od jednej matice k druhej sa deje pomocou invertibilnej matice prechodu od jednej báze k druhej, označme ju T. Potom platí, že maticu lineárneho operátoru f vzhľadom k báze B' dostaneme z matice lineárneho operátoru f vzhľadom k báze B takto: $A_{B'} = TA_BT^{-1}$.

V takom prípade matice $A_{B'}$ a A_B voláme *podobné matice*, značíme $A_{B'} \sim A_B$ (resp. *permutačne podobné*, ak je T permutačná matica, odpovedajúca nejakej permutácií π, ktorej riadky sú práve prepermutované riadky jednotkovej matice permutáciou π, značíme $A_{B'} \sim_\pi A_B$).

V ďalšej časti budeme skúmať násobenie prvkom α telesa $F_{2^n}^*$ reprezentovaného pomocou matice.

Značenie 1.11. *Matica $M_{\alpha,B}$ bude označovať maticu stupňa n reprezentujúcu násobenie (z ľava) prvkom $\alpha \in F_{2^n}^*$ vzhľadom k báze B.*

Nasledujúci diagram nám názorne ukazuje, ako násobenie maticou reprezentujúcou prvok α funguje.



Čo vlastne diagram vyššie hovorí? Majme ľubovoľný prvok $\beta \in F_{2^n}^*$. Chceme β vynásobiť prvkom $\alpha \in F_{2^n}^*$. Lineárny operátor daný násobením prvku α máme reprezentovaný pomocou matice $M_{\alpha,B}$. Preto najprv určíme súradnice β vzhľadom k báze B vektorového priestoru F_2^n pomocou zobrazenia Φ_B. Následne stačí vynásobiť $M_{\alpha,B} \cdot \Phi_B(\beta)$ a inverzným zobrazením k zobrazeniu Φ_B dostaneme hľadaný výsledok.

Ako už bolo spomenuté vyššie, zmenou báze z B na B' sa zmení aj matica $M_{\alpha,B}$ a to ako $M_{\alpha,B'} = TM_{\alpha,B}T^{-1}$, kde T je matica prechodu od báze B k báze B'.

V ďalšej časti práce si pripomenieme pojem minimálneho a charakteristického polynómu matice, a uvedieme niektoré ich užitočné vlastnosti.

Definícia 1.12. (Charakteristický polynóm matice) Charakteristickým polynómom matice A *rozumieme* $\chi_A := \det(\lambda I - A) \in \mathbb{F}_2[\lambda]$.

(Minimálny polynóm matice) Minimálny polynóm matice A *je monický polynóm* p *najnižšieho možného stupňa taký, že* $p(A) = \mathbf{0}_n$. *Budeme ho značiť* m_A.

Nasledujú niektoré dôležité vlastnosti minimálneho a charakteristického polynómu, s ktorými budeme pracovať.

Veta 1.13. (Cayley-Hamilton) *Pre ľubovoľnú maticu* $A \in Mat_n(\mathbb{F})$ *platí, že* $\chi_A(A) = 0$, *teda, že matica* A *je koreňom svojho charakteristického polynómu.*

Dôkaz. Dôkaz je uvedený v práci Zlatoš (2011, Veta 21.1.4., str. 437). □

Lemma 1.14. *Minimálny polynóm matice vždy delí charakteristický polynóm danej matice (*$m_A \mid \chi_A$ *pre maticu maticu* $A \in Mat_n(\mathbb{F})$*).*

Dôkaz. Dôkaz je uvedený v práci Zlatoš (2011, Veta 21.2.2., str. 441). □

Lemma 1.15. *Pre podobné matice platí, že majú rovnaký charakteristický aj minimálny polynóm.*

Dôkaz. Tvrdenie o minimálnych polynómoch plynie z dôkazu tvrdenia v práci Zlatoš (2011, Tvrdenie 21.2.1., str. 441) a diskusie pred ňou.

Dôkaz zhodnosti charakteristických polynómov podobných matíc A a A' dáva nasledujúca rovnosť, kde priamo využívame definíciu charakteristického polynómu a vlastnosť determintantu inverznej matice. Platí

$$\begin{aligned}\det(xI - A') &= \det(xI - M^{-1}AM) = \det(M^{-1}xIM - M^{-1}AM) = \\ &= \det(M^{-1}(xI - A)M) = \det(M^{-1})\det(xI - A)\det(M) = \\ &= \det(xI - A),\end{aligned}$$

kde M je invertibilná matica splňujúca $A' = M^{-1}AM$.

□

Ďalej definujeme jeden špeciálny typ matice, ktorý je kľúčový pre celú prácu, jedná sa o doprovodnú maticu polynómu.

Definícia 1.16. (Doprovodná matica polynómu) *Majme polynóm* $q(x) = x^n + q_{n-1}x^{n-1} + \cdots + q_1x + q_0 \in \mathbb{F}_2[x]$ *stupňa* n. Doprovodnú maticu polynómu q *definujeme ako*

$$C_q = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & q_0 \\ 1 & 0 & 0 & \dots & 0 & q_1 \\ 0 & 1 & 0 & \dots & 0 & q_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & 0 & q_{n-2} \\ 0 & \dots & 0 & 0 & 1 & q_{n-1} \end{pmatrix}.$$

Ďalej pripomenieme pojem racionálnej kanonickej formy matice. Navyše uvedieme tvrdenie, že každá matica je podobná nejakej matici v racionálnej kanonickej forme.

Definícia 1.17. (Racionálna kanonická forma) *Povieme, že matica A je v* racionálnej kanonickej forme*, ak je to blokovo diagonálna matica so štvorcovými maticami na diagonále a tieto matice sú doprovodné matice polynómov $q_1(x), \dots, q_d(x)$ stupňa väčšieho alebo rovného 1 a platí $q_1(x) \mid q_2(x) \mid \dots \mid q_d(x)$.*

Veta 1.18. *Nech $A \in Mat_n(\mathbb{F}_2)$. Potom matica A je podobná práve jednej matici v racionálnej kanonickej forme.*

Dôkaz. Dôkaz je uvedený v práci Hoffman a Kunze (1971, Theorem 5, str. 238).

□

Pripomeňme ešte jednu zásadnú vlastnosť doprovodných matíc polynómu.

Lemma 1.19. *Nech C_q je doprovodná matica polynómu $q(x) \in \mathbb{F}_2[x]\backslash\{0\}$. Potom charakteristický aj minimálny polynóm matice C_q sú zhodné s polynómom $q(x)$, zapísané v symboloch $\chi_{C_q} = m_{C_q} = q$.*

Dôkaz. Dôkaz je uvedený v práci Bečvář (2005, Lemma 18.27, str. 257).

□

Dá sa povedať, že matica A je podobná doprovodnej matici polynómu práve vtedy, keď je jej charakteristický a minimálny polynóm rovnaký. V tomto prípade je matica C_q racionálnou kanonickou formou matice A.

Na záver tejto sekcie uveďme ešte jednu špeciálnu maticu.

Definícia 1.20. (Blokovo horná (dolná) trojuholníková matica) *Povieme, že matica A stupňa n je* bloková horná trojuholníková matica*, ak je v tvare*

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & \dots & A_{1,l} \\ \mathbf{0} & A_{2,2} & \dots & A_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{0} & \dots & \mathbf{0} & A_{l,l} \end{pmatrix},$$

kde $A_{i,j}$ sú matice stupňa $\leq n$, na diagonále sú štvorcové, $i, j \in \{1, \dots, l\}$, $i \leq j$, $l \leq n$.

Bloková dolná trojuholníková matica *sa definuje obdobne, ale platí $i \geq j$.*

1.3 Počet XOR operácií

Doteraz sme sa venovali viac známym veciam z algebry a z konečných telies. V tejto časti sa už dostaneme k teórií, ktorá patrí skôr do kryptografie. Pozrieme sa na definíciu počtu XOR operácií a uvedieme niekoľko pozorovaní, ktoré obsahujú užitočné vlastnosti využiteľné pri určení počtu XOR operácií potrebných na implementáciu fixného prvku konečného telesa.

Na začiatok sa zameráme na definíciu počtu XOR operácií.

Pripomeňme, že pod pojmom XOR v telese $\mathbb{F}_2$ rozumieme operáciu sčítania.

Uveďme jedno pomocné tvrdenie.

Lemma 1.21. *Nech A je regulárna matica stupňa n nad telesom $\mathbb{F}_2$. Potom sa dá matica A zapísať v tvare*

$$A = P + \sum_{k=1}^{t} E_{i_k,j_k} \tag{1.1}$$

kde $E_{i_k,j_k} \neq E_{i_l,j_l}$, $k, l \in \{1, \dots, t\}$, $k \neq l$, platí, že $wt(A) = n+t$, P je permutačná matica a t je najmenšie celé číslo také, že matica A sa dá v tomto tvare zapísať.

Dôkaz. Matica v tvare z rovnosti (1.1) je vlastne permutačnou maticou s t pridanými nenulovými prvkami. Stačí dokázať, že sa dá z matice A vybrať nejaká permutačná matica P. Ostatné nenulové prvky matice budú dané t maticami E_{i_k,j_k}.

Budeme dokazovať induktívne takto:

Keďže je matica A regulárna, má nenulový determinant. Tento determinant môžeme spočítať rozvojom podľa prvého riadku matice A. Keďže je determinant nenulový, tak v prvom riadku matice musí byť aspoň jeden nenulový prvok, ktorého subdeterminant (ktorý sa spočíta ako determinant matice vzniknutej z

matice A vynechaním prvého riadku a stĺpca, v ktorom sa vybraný nenulový prvok nachádza) je nenulový. Ľubovoľný takýto prvok v prvom riadku zvolíme ako prvok hľadanej permutačnej matice. Našli sme tak prvý prvok permutačnej matice, ktorý bude v permutačnej matici stupňa n v prvom riadku a v rovnakom stĺpci ako v matici A.

Hľadanie ďalších prvkov permutačnej matice P prebieha induktívne tak, že si vezmeme príslušnú submaticu (získanú z matice z predchádzajúceho kroku vynechaním stĺpca a riadku, z ktorých sme volili prvok do permutačnej matice) a opakujeme postup ako pri hľadaní prvého prvku permutačnej matice aplikovaný na túto submaticu.

V druhom kroku teda hľadáme prvok permutačnej matice v prvom riadku matice stupňa $n-1$. Po zvolení ďalšieho prvku permutačnej matice sa musíme pozrieť, na akej pozícií bol tento prvok v pôvodnej matici a na túto pozíciu ho umiestníme do hľadanej permutačnej matice.

Keďže je matica regulárna, môžeme takto pokračovať až prevedieme práve n krokov a vo výsledku získame permutačnú maticu stupňa n.

Ostatné nenulové prvky matice A, ktoré nie sú obsiahnuté v matici P, budú definované maticami E_{i_k,j_k}, $k \in \{1,\dots,t\}$, i_k, $j_k \in \{1,\dots,n\}$, ktoré sú navzájom rôzne a nemajú nenulový prvok na mieste, kde je nenulový prvok v matici P.

□

Na príklade si ukážeme, ako funguje hľadanie permutačnej matice z dôkazu predchádzajúcej vety.

Príklad 1.22. *Majme regulárnu maticu*

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Našou úlohou je nájsť permutačnú maticu P a matice E_{i_k,j_k}, k, i_k,$j_k \in \{1,\dots,3\}$, pomocou ktorých sa dá matica A zapísať ako v rovnosti (1.1). Budeme postupovať tak, ako bolo naznačené v dôkaze lemma 1.21.

Počítame teda determinant matice rozvojom podľa prvého riadku v $\mathbb{F}_2$:

$$\begin{vmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 1 \\ 0 & 0 \end{vmatrix} + 0 \cdot \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} + 1 \cdot \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}$$

Jediný nenulový člen tohto súčtu je ten posledný. Preto bude permutačná matica P obsahovať v prvom riadku jednotku v 3. stĺpci.

Na hľadanie druhého prvku permutačnej matice počítame determinant submatice

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

ktorá vznikla z matice A vynechaním 1. riadku a 3. stĺpca.

Počítame:

$$\begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix} = 1 \cdot 0 + 1 \cdot 1.$$

Nenulový príspevok do súčtu je len z druhého sčítanca a preto ako druhý nenulový prvok P volíme prvok v 2. riadku a 2. stĺpci matice A.

Zrejme nám ostane matica stupňa 1 a to práve prvok v 1. stĺpci a 3. riadku matice A, ktorý bude posledným hľadaným nenulovým prvkom permutačnej matice P.

Dostávame teda, že

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

a platí:

$$A = P + E_{1,1} + E_{2,1} + E_{2,3}.$$

V starších prácach, ktoré sa venovali tejto problematike (napríklad v práci Sim a kol. (2015)), sa počet XOR operácií pre maticu A stupňa n definoval ako to najmenšie t, ktoré splňovalo rovnosť (1.1) z lemma 1.21.

Táto definícia počtu XOR operácií má jeden zásadný nedostatok. Problém je v tom, že síce všetky matice, ktoré túto definíciu spĺňajú sa dajú implementovať s nanajvýš t XOR-mi, ale táto definícia nám nedáva všetky možné matice, ktoré by sa dali implementovať maximálne s t XOR operáciami.

Nasledujúci príklad nám ukáže, čo to v praxi znamená.

Príklad 1.23. *Existujú matice, ktoré majú 3 pridané nenulové prvky, ale dajú sa implementovať len s dvoma XOR-mi. Napríklad*

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} v_1 + v_3 \\ (v_1 + v_3) + v_2 \\ v_3 \end{pmatrix}.$$

Vidíme, že v druhom riadku stačí použiť XOR operáciu na výsledok XOR operácie z prvého riadku a prvku v_2.

Z toho vyplýva, že podľa definície počtu XOR operácií, využívanej v starších prácach, by sme pre maticu z predchádzajúceho príkladu dostali, že má počet XOR operácií 3, aj keď v skutočnosti na jej implementáciu stačia len 2 XOR operácie.

Preto uvedieme vhodnejšiu definíciu počtu XOR operácií.

Definícia 1.24. (Počet XOR operácií) *Povieme, že invertibilná matica A reprezentuje* počet XOR operácií *t, keď t bude najmenšie číslo také, že sa dá matica A zapísať ako*

$$A = P \prod_{k=1}^{t} (I + E_{i_k,j_k}), \tag{1.2}$$

kde $i_k \neq j_k$ pre všetky $k \in \{1, \ldots, t\}$ a P je permutačná matica.

Počet XOR operácií danej matice budeme značiť $wt_{\oplus}(A) = t$.

Príklad 1.25. *Ukážeme, ako by v našej definícií počtu XOR operácií vyzerala daná matica z príkladu 1.23.*

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix} = P(I + E_{2,3})(I + E_{3,1}),$$

kde

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

A teda podľa definície 1.24 reprezentuje matica A počet XOR operácií 2.

Príklad nám názorne ukazuje, že reprezentácia matice uvedená v definícií 1.24 skutočne dáva horný odhad na počet XOR operácií, ktorý reprezentuje daná matica.

Upozornime na to, že definícia 1.24 počíta počet XOR-ov len bez použitia dočasných registrov, ktoré by inak mohli znížiť počet XOR-ov. Definícia používaná v starších textoch umožňovala použitie dočasných registrov. Pre matice s počtom XOR-ov menším alebo rovným 2 však obmedzenie použitia dočasných registrov nemá vplyv. To sú práve prípady, ktoré nás najviac zaujímajú.

V nasledujúcej poznámke sa pozrieme na porovnanie oboch definícií počtu XOR operácií pre t rovno 1 a 2.

Poznámka 1.26. *Definícia 1.24 sa zhoduje so staršou definíciou pre prípad* $t = 1$*. V ostatných prípadoch počet pridaných nenulových prvkov matice (v zmysle najmenšieho t použitého v rovnosti (1.1)) rastie s rastúcim t. V našej práci nás bude okrem prípadu* $t = 1$ *zaujímať aj prípad* $t = 2$*. Po vyhodnotení súčinu matíc v definícií 1.24 vidíme, že matica A, pre ktorú platí* $wt_{\oplus}(A) = 2$*, má tvar*

$$A = \begin{cases} P + P(E_{i_1,j_1} + E_{i_2,j_2}) & ak\ i_2 \neq j_1 \\ P + P(E_{i_1,j_1} + E_{i_2,j_2} + E_{i_1,j_2}) & ak\ i_2 = j_1 \end{cases}.$$

Rozdelenie na 2 prípady podľa toho, či sú i_2 *a* j_1 *rovnaké alebo nie, je z toho dôvodu, že pokiaľ sú rovnaké, tak pri násobení matíc* $(I + E_{i_1,j_1})(I + E_{i_2,j_2})$ *je výsledkom matica s tromi pridanými nenulovými prvkami k jednotkovej matici (čo je dôsledok spôsobu, akým sa matice násobia), v opačnom prípade je výsledkom matica s dvoma pridanými nenulovými prvkami.*

Nasledujúce lemma a tvrdenie nám priblížia v akom vzťahu je počet XOR-ov matice s počtom XOR-ov matice permutačne podobnej a matice inverznej.

Lemma 1.27. *Nech* $A \in Mat_n(\mathbb{F}_2)$ *je invertibilná matica a nech matica* A' *je permutačne podobná matici A, teda platí* $A' = QAQ^{-1}$ *pre permutačnú maticu Q reprezentujúcu permutáciu* $\pi \in S_n$*, ktorá permutuje riadky matice. Potom* $wt_{\oplus}(A) = wt_{\oplus}(A')$*.*

Navyše, ak $A = P\prod_{k=1}^{t}(I+E_{i_k,j_k})$*, potom* $A' = QPQ^{-1}\prod_{k=1}^{t}(I+E_{\pi(i_k),\pi^{-1}(j_k)})$*, kde* $i_k \neq j_k$ *pre všetky* $k \in \{1,\ldots,t\}$ *a P je permutačná matica.*

Dôkaz. Nech $A' = QAQ^{-1}$, kde Q je permutačná matica reprezentujúca permutáciu $\pi \in S_n$. Nech $I + E_{i_k,j_k}$ je člen reprezentácie počtu XOR operácií matice $A = P\prod_{k=1}^{t}(I + E_{i_k,j_k})$, kde $t = wt_{\oplus}(A)$. Potom platí nasledujúca rovnosť:

$$(I + E_{i_k,j_k})Q^{-1} = Q^{-1} + E_{i_k,\pi^{-1}(j_k)} = Q^{-1}(I + E_{\pi(i_k),\pi^{-1}(j_k)}).$$

Ak rovnakú úpravu prevedieme postupne vo všetkých členoch, dostaneme výraz

$$\begin{aligned}
A' = QAQ^{-1} &= QP\prod_{k=1}^{t}(I+E_{i_k,j_k})Q^{-1} = \\
&= QPQ^{-1}Q(I+E_{i_1,j_1})\dots Q^{-1}Q(I+E_{i_{t-1},j_{t-1}})Q^{-1}Q(I+E_{i_t,j_t})Q^{-1} = \\
&= QPQ^{-1}Q(I+E_{i_1,j_1})\dots Q^{-1}Q(I+E_{i_{t-1},j_{t-1}})Q^{-1}(I+E_{\pi(i_t),\pi^{-1}(j_t)}) = \\
&= QPQ^{-1}Q(I+E_{i_1,j_1})\dots Q^{-1}(I+E_{\pi(i_{t-1}),\pi^{-1}(j_{t-1})})(I+E_{\pi(i_t),\pi^{-1}(j_t)}) = \\
&= \dots = \\
&= QPQ^{-1}\prod_{k=1}^{t}(I+E_{\pi(i_k),\pi^{-1}(j_k)}).
\end{aligned}$$

Matica QPQ^{-1} je permutačná matica, preto rovnosť

$$A' = QPQ^{-1}\prod_{k=1}^{t}(I+E_{\pi(i_k),\pi^{-1}(j_k)})$$

znamená, že A' sa dá zapísať v tvare z rovnosti (1.2). Pre maticu A' by však nemuselo platiť, že dané t je práve to najmenšie možné, aby sa matica v takomto tvare dala zapísať. Preto platí: $wt_{\oplus}(A) \geq wt_{\oplus}(A')$.

Všimnime si, že opačná nerovnosť plynie z toho, že môžeme uvažovať $A = Q^{-1}A'Q$ a podobnými úvahami, ako v prvej časti dôkazu, dostaneme požadovanú nerovnosť $wt_{\oplus}(A) \leq wt_{\oplus}(A')$.

Tým je lemma dokázané, teda platí $wt_{\oplus}(A) = wt_{\oplus}(A')$.

□

Veta 1.28. (Počet XOR operácií inverznej matice) *Nech A je invertibilná matica, pre ktorú platí $wt_{\oplus}(A) = t$. Potom platí $wt_{\oplus}(A^{-1}) = t$.*

Dôkaz. Nech $A = P\prod_{k=1}^{t}(I+E_{i_k,j_k})$, kde $i_k \neq j_k$ pre všetky $k \in \{1,\dots,t\}$ a P je permutačná matica. Stačí dokázať, že A^{-1} je permutačne podobná matici s počtom XOR operácií rovným $wt_{\oplus}(A) = t$. To plynie z nasledujúcej rovnosti:

$$A^{-1} = \Big(P\prod_{k=1}^{t}(I+E_{i_k,j_k})\Big)^{-1} = \Big(\prod_{k=t}^{1}(I+E_{i_k,j_k})\Big)P^{-1} \sim_{\pi} P^{-1}\prod_{k=t}^{1}(I+E_{i_k,j_k}).$$

Využitím lemma 1.27 a toho, že P^{-1} je tiež permutačná matica, dostávame, že skutočne platí $wt_{\oplus}(A^{-1}) = t$.

□

Pre potreby hľadania všetkých matíc danej dimenzie n s nízkym počtom XOR operácií potrebných na implementáciu by sa nám hodila permutačná matica P v špecifickom tvare. Tento špecifický tvar matice nám ušetrí výpočtovú náročnosť hľadania, pretože s rastúcim n rapídne stúpa aj počet možností na voľbu permutačnej matice (pre dané n je počet možností $n!$).

Lemma 1.29. *Pre permutačnú maticu P stupňa n platí*

$$P \sim_{\pi} \bigoplus_{k=1}^{d} C_{x^{m_k}+1}, \tag{1.3}$$

pre nejaké $m_k \in \mathbb{N}$ také, že $\sum_{k=1}^{d} m_k = n$ a $m_1 \geq m_2 \geq \dots \geq m_d \geq 1$.

Dôkaz. Z definície doprovodnej matice polynómu (definícia 1.16) má matica $C_{x^{m_k}+1}$ stupňa m_k tvar

$$C_{x^{m_k}+1} = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}.$$

Je to teda permutačná matica. Spojením d takýchto permutačných matíc do blokovo diagonálnej matice získame opäť permutačnú maticu.

Ostáva ukázať, že každá permutačná matica sa dá v tomto tvare zapísať. Využijeme vlastnosť, že ak majú dve permutácie rovnaký cyklický zápis, tak sú konjugované (dôkaz tejto vlastnosti sa dá nájsť v knihe Dummit a Foote (2004, Proposition 11, str. 126)). Teda pre permutácie ϕ, $\lambda \in S_n$ s rovnakým cyklickým zápisom existuje permutácia $\pi \in S_n$ tak, že platí: $\pi\phi\pi^{-1} = \lambda$.

Nech teda ϕ značí permutáciu definovanú maticou P. Potom existuje permutácia π tak, že

$$\pi\phi\pi^{-1} = (d_1,1,2,\dots,d_1-1)(d_2,d_1+1,\dots,d_2-1)\dots(d_m,d_{m-1}+1,\dots,d_m-1).$$

Stačí si uvedomiť, že tento cyklický zápis presne odpovedá tvaru permutačnej matice $\bigoplus_{k=1}^{d} C_{x^{m_k}+1}$.

Pre lepšie pochopenie predchádzajúceho zápisu si predstavme, že máme nejakú n-prvkovú množinu zapísanú ako vektor

$$d = (1,2,\dots,d_1,d_1+1,d_1+2,\dots,d_{m-1},d_{m-1}+1,\dots,d_m),$$

ktorú chceme permutovať pomocou permutačnej matice v tvare $\bigoplus_{k=1}^{d} C_{x^{m_k}+1}$. Permutácia teda zobrazí prvok d_1 na 1, prvok 1 na 2, ..., prvok $d_1 - 1$ na d_1. Podobne pre všetky ostatné cykly danej permutácie.

Ak teda permutáciu π reprezentujeme maticou Q, tak požadovaný tvar permutačnej matice z matice P dostaneme ako QPQ^{-1}.

□

Tvar matice z predchádzajúceho tvrdenia si zadefinujeme ako cyklickú normálnu formu matice.

Definícia 1.30. (Cyklická normálna forma) *Povieme, že permutačná matica P je v* cyklickej normálnej forme*, ak je táto matica v tvare z lemma 1.29, teda v tvare*

$$\bigoplus_{k=1}^{d} C_{x^{m_k}+1},$$

pre nejaké $m_k \in \mathbb{N}$ také, že $\sum_{k=1}^{d} m_k = n$ a $m_1 \geq m_2 \geq \dots \geq m_d \geq 1$.

Cyklickú normálnu formu matice P budeme označovať $C(P)$.

Až na permutačnú ekvivalenciu môžeme predpokladať, že permutačná matica P danej matice A s $wt_{\oplus}(A) = t$ je v cyklickej normálnej forme. Túto skutočnosť dokazuje nasledujúca veta.

Veta 1.31. *Majme maticu $A \in Mat_n(\mathbb{F}_2)$, pre ktorú platí $wt_\oplus(A) = t$ a je v tvare $A = P\prod_{k=1}^{t}(I + E_{i_k,j_k})$, kde $i_k \neq j_k$ pre všetky $k \in \{1,\ldots,t\}$ a P je permutačná matica. Potom platí*

$$A \sim_\sigma C(P)\prod_{k=1}^{t}(I + E_{\sigma(i_k),\sigma^{-1}(j_k)}),$$

pre nejakú permutáciu $\sigma \in S_n$.

Dôkaz. Z lemma 1.29 vieme, že existuje permutačná matica Q reprezentujúca permutáciu σ tak, že $QPQ^{-1} = C(P)$. Potom matica QAQ^{-1} je permutačne podobná matici A, preto z lemma 1.27 dostávame, že

$$A \sim_\sigma C(P)\prod_{k=1}^{t}(I + E_{\sigma(i_k),\sigma^{-1}(j_k)}).$$

Tým dostávame požadovanú permutačnú ekvivalenciu.

□

2. Efektívne násobenie v konečnom telese

V tejto kapitole sa pozrieme na to, ako sa dá čo najefektívnejšie násobiť prvkom konečného telesa, ktorý je reprezentovaný pomocou matice. Pozrieme sa na to, za akých podmienok nejaká matica reprezentuje násobenie prvkom konečného telesa. A nakoniec budeme skúmať, ktoré prvky konečného telesa sa dajú implementovať s 1 alebo 2 XOR operáciami.

2.1 Násobenie prvkom konečného telesa reprezentovaného maticou

Na začiatok uvedieme niekoľko výsledkov na pochopenie štruktúry matíc $M_{\alpha,B}$, ktoré reprezentujú násobenie s prvkom konečného telesa $\alpha \in \mathbb{F}_{2^n}^*$ vzhľadom k báze B telesa $\mathbb{F}_{2^n}$ ako n-dimenzionálneho vektorového priestoru nad $\mathbb{F}_2$.

Uvedieme niekoľko pomocných tvrdení, ktoré budeme potrebovať na dôkaz vety 2.4.

Lemma 2.1. *Nech $A \in Mat_n(\mathbb{F}_2)$. Potom podokruh okruhu $Mat_n(\mathbb{F}_2)$ generovaný maticou A definuje teleso s 2^n prvkami práve vtedy, keď charakteristický polynóm χ_A je ireducibilný stupňa n.*

Dôkaz. Tvrdenie plynie z úvah v práci Wardlaw (1994, diskusia na strane 291). □

Lemma 2.2. *Nech $A \in Mat_n(\mathbb{F}_2)$ je matica s ireducibilným minimálnym polynómom. Potom charakteristický polynóm χ_A matice A je mocninou minimálneho polynómu m_A. Teda pre nejaké $d \in \mathbb{N}$ platí $\chi_A = (m_A)^d$.*

Dôkaz. Tvrdenie platí vďaka tomu, že oba polynómy majú rovnaké ireducibilné činitele (to je dokázané v práci Conrad, Corollary 4.10., str. 6) a keďže je m_A ireducibilný polynóm, inak povedané má jediný ireducibilný činiteľ, tak aj charakteristický polynóm má jediný ireducibilný činiteľ. Charakteristický polynóm však môže mať väčší stupeň ako minimálny polynóm a preto je mocninou minimálneho polynómu.

□

Lemma 2.3. *Nech A je blokovo trojuholníková matica. Potom charakteristický polynóm χ_A matice A je práve súčinom charakteristických polynómov blokov na diagonále.*

Dôkaz. Tvrdenie je uvedené ako cvičenie v skriptách Barto a Tůma (2014, Cvičenie 9., str. 239).

□

Všimnime si, že počet XOR operácií potrebných k implementácií matice $M_{\alpha,B}$ je závislý na voľbe bázy B.

Z vety 1.31 vieme, že môžeme maticu s daným počtom XOR operácií predpokladať v určitej normovanej forme.

Je potrebné si uvedomiť, že nie všetky matice reprezentujú násobenie v konečnom telese. Na určenie toho, ktoré matice reprezentujú násobenie prvkom konečného telesa α nám dáva dobrý pohľad nasledujúca veta, ktorá nám dovoľuje rýchlo rozhodnúť o tom, či daná matica reprezentuje nejaké násobenie. Hlavnou myšlienkou je využiť minimálny polynóm prvku α, ktorý je vlastnosťou lineárneho zobrazenia

$$f_\alpha \colon \mathbb{F}_{2^n} \longmapsto \mathbb{F}_{2^n},\ \beta \longmapsto \alpha\beta$$

a to je nezávislé na zmene reprezentácie f_α v inej báze.

Veta 2.4. *Nech $A \in Mat_n(\mathbb{F}_2)\backslash\{\mathbf{0}_n\}$. Potom pre nejaké $\alpha \in \mathbb{F}^*_{2^n}$ a vzhľadom na bázu B je $A = M_{\alpha,B}$ práve vtedy, keď m_A je ireducibilný polynóm.*

Dôkaz. Majme maticu $A \in Mat_n(\mathbb{F}_2)\backslash\{\mathbf{0}_n\}$. Podokruh okruhu $Mat_n(\mathbb{F}_2)$ generovaný $\mathbb{F}_2 \cup A$ má tvar: $\mathbb{F}_2[A] = \{\sum_{i=0}^{n-1} \alpha_i A^i \mid \alpha_i \in \mathbb{F}_2\}$, pretože A^n sa dá vyjadriť ako lineárna kombinácia $A^0, \ldots, A^{n-1}$. Z lemma 2.1 vieme, že okruh $\mathbb{F}_2(A)$ definuje teleso s 2^n prvkami práve vtedy, keď charakteristický polynóm χ_A je ireducibilný stupňa n. Vďaka vete 1.13 vieme, že platí $\chi_A(A) = 0$ a teda matica A je koreňom polynómu stupňa n.

Na to, aby okruh $\mathbb{F}_2(A)$ bol telesom, nemusí mať matica A ireducibilný charakteristický polynóm. V takom prípade môže matica A generovať nejaké podteleso $\mathbb{F}_{2^m}$ telesa $\mathbb{F}_{2^n}$. Ukážeme, že taký prípad nastáva práve vtedy, keď m_A je ireducibilný polynóm stupňa $m < n$ (dokonca m delí n).

Ak m_A nie je ireducibilný, potom existujú polynómy $u, v \in \mathbb{F}_2[x]$ stupňa menšieho než $\deg(m_A)$, pre ktoré platí $m_A = u \cdot v$, $u(A) \neq 0 \neq v(A)$ a $u(A) \cdot v(A) = m_A(A)$. Preto $\mathbb{F}_2(A)$ nie je obor a teda nie je ani teleso, preto matica A nemôže reprezentovať násobenie v telese.

Nech je teda m_A ireducibilný polynóm. Charakteristický polynóm χ_A je potom mocninou m_A, teda pre nejaké $d \in \mathbb{N}$ platí $\chi_A = (m_A)^d$ (platí vďaka lemma 2.2). Potom d aj $\deg(m_A)$ delia n. Keďže m_A je ireducibilný polynóm, tak racionálna kanonická forma matice A sa skladá z d blokov tvaru C_{m_A}, teda

$$A \sim \bigoplus_{k=1}^{d} C_{m_A}.$$

To, že sa dá matica A zapísať v tvare racionálnej kanonickej formy plynie z vety 1.18. To, že racionálna kanonická forma má práve takýto tvar plynie z toho, že matica A a jej racionálna kanonická forma, musia mať rovnaký charakteristický polynóm a keďže vieme, že charakteristický polynóm je mocninou minimálneho polynómu, teda $\chi_A = (m_A)^d$ tak jediná možnosť na voľbu racionálnej kanonickej formy je $\bigoplus_{k=1}^{d} C_{m_A}$. Charakteristický polynóm matice $\bigoplus_{k=1}^{d} C_{m_A}$ je práve súčin charakteristických polynómov matíc C_{m_A} (plynie z lemma 2.3). Skutočne má teda rovnaký charakteristický polynóm ako matica A.

Z lemma 1.19 vieme, že charakteristický polynóm doprovodnej matice nejakého polynómu je práve daný polynóm. V našom prípade teda platí $\chi_{C_{m_A}} = m_A$

a vďaka ireducibilite m_A, vieme, že matica A reprezentuje násobenie prvkom konečného telesa v nejakom podtelese telesa $\mathbb{F}_{2^n}$.

□

Poznamenajme, že pre každé α je $m_\alpha = m_A$, kde A je matica reprezentujúca násobenie prvkom α. Preto pre maticu A je identifikácia prvku α, pre ktorý je $A = M_{\alpha,B}$ ekvivalentná určeniu minimálneho polynómu matice A. Matica A je v tomto prípade podobná matici C_{m_α} a tá má skutočne minimálny polynóm rovný m_α.

2.2 Prvky s najnižším počtom XOR operácií

Hlavné otázky, ktoré si potrebujeme položiť, sú, ktoré prvky konečného telesa sa dajú implementovať s minimálnym počtom XOR operácií a aký počet XOR-ov potrebujeme na implementáciu konkrétneho prvku $\alpha \in \mathbb{F}^*_{2^n}$.

Triviálne odpovede sú: na prvú otázku je triviálna odpoveď $\alpha = 1$ (na túto implementáciu nepotrebujeme žiadnu XOR operáciu, pretože $M_{\alpha,B} = I_n$ pre všetky bázy B) a na druhú otázku je to počet XOR operácií 0 a to v prípade, že sa jedná o prvok 1.

Potrebujeme sa teda ešte pozrieť, ako je to s netriviálnymi prípadmi. Nasledujúca veta nám dáva nevyhnutnú podmienku na minimálny polynóm prvku α, aby na implementáciu násobenia prvkom α stačila 1 XOR operácia.

Veta 2.5. *Nech $\alpha \in \mathbb{F}^*_{2^n}$, potom existuje matica A stupňa n taká, že $wt_\oplus(A) = 1$ a $A = M_{\alpha,B}$ pre nejakú bázu B práve vtedy, keď m_α je ireducibilný trojčlen stupňa n.*

Dá sa zvoliť báza B tak, že matica $M_{\alpha,B}$ je v tomto prípade v špeciálnom tvare $M_{\alpha,B} = C_{x^n+1} + E_{i,j}$.

Dôkaz. Najprv dokážeme implikáciu z ľava do prava. Majme teda maticu $M_{\alpha,B}$ stupňa n, ktorá reprezentuje násobenie prvkom $\alpha \in \mathbb{F}^*_{2^n}$ vzhľadom k báze $B = (b_0, \ldots, b_{n-1})$. Predpokladajme, že $wt_\oplus(M_{\alpha,B}) = 1$. Ukážeme, že $\chi_{M_{\alpha,B}}$ je trojčlen stupňa n a zároveň $\chi_{M_{\alpha,B}} = m_\alpha$.

Keďže platí, že $wt_\oplus(M_{\alpha,B}) = 1$, tak môžeme bez straty na všeobecnosti výpočtu z definície počtu XOR operácií predpokladať špeciálny tvar $M_{\alpha,B} = P + E_{i,j}$ tak, že $P = \bigoplus_{k=1}^{d} C_{x^{m_k}+1}$, kde platí $\sum_{k=1}^{d} m_k = n$. Permutačná matica P je teda v cyklickej normálnej forme a to, že maticu P môžeme predpokladať v takom tvare plynie z lemma 1.29. Stĺpce a riadky matice $M_{\alpha,B}$ budeme indexovať od 0 do $n-1$ a tiež v matici $E_{i,j}$ budú $i, j \in \{0, \ldots, n-1\}$.

Najprv ukážeme, že $d = 1$. Teda, že permutačná matica P je v tvare doprovodnej matice polynómu x^n+1. Predpokladajme pre spor, že $d > 1$. Potom v závislosti na tvare matice $E_{i,j}$ je matica $M_{\alpha,B}$ horná alebo dolná blokovo trojuholníková matica s minimálne dvoma blokmi na diagonále. Jediný nenulový prvok matice $E_{i,j}$ bude buď mimo matíc na diagonále alebo padne práve do jednej z týchto matíc. Preto môžeme predpokladať, že jeden z týchto blokov, ten, do ktorého nenulový prvok matice $E_{i,j}$ nepadol, má tvar C_{x^m+1}. Potom z lemma 2.3 polynóm $x^m + 1$ musí deliť charakteristický polynóm matice $M_{\alpha,B}$ (teda $(x^m + 1) \mid \chi_{M_{\alpha,B}}$). Zároveň platí $(x + 1) \mid (x^m + 1)$, z čoho plynie, že minimálny polynóm α je násobkom

polynómu $x+1$. Ale to je spor s tým, že $\alpha \neq 1$ a m_α má byť ireducibilný polynóm. Preto $d = 1$ a platí $M_{\alpha,B} = C_{x^n+1} + E_{i,j}$, kde $i \neq j+1 \mod n$, inak by bola matica $M_{\alpha,B}$ singulárna.

Pozrime sa na to, ako násobenie prvkom α pôsobí na prvky báze B. Využitím štruktúry matice

$$M_{\alpha,B} = C_{x^n+1} + E_{i,j} = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix} + E_{i,j},$$

kde $E_{i,j}$ je matica s jednotkou v i-tom riadku a j-tom stĺpci, dostaneme nasledujúce rovnosti

$$\begin{aligned} \alpha b_0 &= b_1 \\ \alpha b_1 &= b_2 \\ &\vdots \\ \alpha b_{j-1} &= b_j \\ \alpha b_j &= b_{j+1} + b_i \\ \alpha b_{j+1} &= b_{j+2} \\ &\vdots \\ \alpha b_{n-1} &= b_0. \end{aligned}$$

Za povšimnutie stojí rovnosť $\alpha b_j = b_{j+1} + b_i$, ktorá vyjadruje vplyv pridanej jednotky matice $E_{i,j}$ na násobenie maticou $M_{\alpha,B}$. Predpokladáme $i \neq j+1 \mod n$, preto je táto rovnosť v poriadku.

Definujeme si pomocnú hodnotu $\gamma := b_{j+1}$. Potom dokážeme každý prvok báze B, vyjadriť ako hodnotu γ vynásobenú mocninou α. Platí

$$b_{j+k} = \alpha^{k-1}\gamma, \tag{2.1}$$

pre $k \in \{1, \dots, n\}$. V indexoch prvkoch báze b_{j+k} v predchádzajúcom vzorci, ale aj v nasledujúcej časti, budeme počítať $j + k \mod n$. Teda počítame nasledujúcim spôsobom, napríklad $b_{j+(n-j+1) \mod n} = b_{n+1 \mod n} = b_1 = \alpha^{n-j}\gamma$.

Spojením predchádzajúcej rovnosti s rovnosťou $\alpha b_j = b_{j+1} + b_i$ tak, že za prvky báze dosadíme ich reprezentáciu pomocou mocniny α prenásobenej γ dostaneme rovnosť

$$\alpha^n\gamma = \gamma + \alpha^t\gamma, \tag{2.2}$$

pre nejaké $t \neq 0$. Napríklad ľavú stranu predchádzajúcej rovnosti sme dostali nasledovne:

$$\alpha b_j = \alpha b_{j+n} = \alpha\alpha^{n-1}\gamma = \alpha^n\gamma.$$

Pretože $\gamma \neq 0$, tak α je koreňom trojčlenu $\gamma x^n - \gamma x^t - \gamma$, po skrátení prvku γ a uvedomení si, že sa jedná o trojčlen nad $\mathbb{F}_2$ dostaneme, že α je koreňom trojčlenu $p = x^n + x^t + 1$.

Ostáva ukázať, že p je práve minimálny polynóm m_α. Predpokladajme pre spor, že $m_\alpha = x^m + \sum_{h=0}^{m-1} c_h x^h$, kde $c_h \in \{0,1\}$ a $m < n$. Vynásobením $m_\alpha(\alpha)$ hodnotou γ dostaneme výraz

$$\alpha^m \gamma = \sum_{h=0}^{m-1} c_h \alpha^h \gamma.$$

Z toho vyplýva, že platí $b_m = \sum_{h=0}^{m-1} c_h b_h$, pre nejaké prvky $b_m, b_h \in B$, $h \in \{0, \ldots, m-1\}$. Dokážeme teda jeden prvok báze vyjadriť ako súčet iných prvkov báze B. To je spor s lineárnou nezávislosťou prvkov báze.

Z toho teda dostávame výsledok, že $\deg(m_\alpha) = n$ a potom $m_\alpha = p$. Tým sme dokázali prvú implikáciu.

Opačná implikácia sa dokáže nasledovne. Majme minimálny polynóm m_α prvku α, ktorý je ireducibilný trojčlen stupňa n. Vezmeme si doprovodnú maticu tohto polynómu. Potom zrejme platí

$$C_{m_\alpha} = C_{x^n+1} + E_{i,n},$$

pre vhodné $i > 1$. Podľa vety 2.4 je $C_{m_\alpha} = M_{\alpha,B}$ pre nejakú bázu B a tento tvar presne spĺňa definíciu počtu XOR operácií, preto platí $wt_\oplus(A) = 1$.

Tým sme tvrdenie dokázali.

□

Poznamenajme, že z dôkazu priamej implikácie z predchádzajúcej vety, je polynóm p tiež charakteristickým polynómom matice $M_{\alpha,B}$, pretože to musí byť monický polynóm a násobok polynómu m_α stupňa n.

Jednoduchým dôsledkom predchádzajúcej vety je, že $\alpha \in \mathbb{F}_{2^n}^*$ s počtom XOR operácií 1 nemôže byť vo vlastnom podtelese telesa $\mathbb{F}_{2^n}$.

Dôsledok 2.6. *Nech $\alpha \in \mathbb{F}_{2^n}^* \backslash \{1\}$ a predpokladajme, že $\deg(m_\alpha) < n$ (čo znamená, že α je vo vlastnom podtelese telesa $\mathbb{F}_{2^n}$). Potom pre maticu $M_{\alpha,B}$ reprezentujúcu násobenie prvkom α vzhľadom ku každej báze B platí $wt_\oplus(M_{\alpha,B}) > 1$.*

Ďalej uvažujme prvok α, násobenie ktorým sa dá implementovať s 1 XOR operáciou. Z vety 1.28 vieme, že na implementáciu násobenia prvkom α^{-1} potrebujeme tiež 1 XOR operáciu. Nasledujúca veta nám ukáže, že už potom v danom telese neexistujú žiadne ďalšie prvky, ktoré by sa dali implementovať s 1 XOR operáciou.

Veta 2.7. *Pre danú bázu B telesa $\mathbb{F}_{2^n}$ existujú najviac 2 prvky daného telesa α a α^{-1}, pre ktoré platí $wt_\oplus(M_{\alpha,B}) = wt_\oplus(M_{\alpha^{-1},B}) = 1$.*

Dôkaz. Majme $\alpha \in \mathbb{F}_{2^n}^*$ prvok, pre ktorý platí $wt_\oplus(M_{\alpha,B}) = 1$ vzhľadom k báze $B = (b_0, \ldots, b_{n-1})$. Dôkaz prevedieme tak, že pre ľubovoľné $\beta \in \mathbb{F}_{2^n}^*$ s vlastnosťou $wt_\oplus(M_{\beta,B}) = 1$ ukážeme, že nutne platí $\beta = \alpha^{\pm 1}$.

Bez ujmy na všeobecnosti výpočtu môžeme predpokladať, že pre nejakú konkrétnu bázu B je matica $M_{\alpha,B}$ v špeciálnom tvare $M_{\alpha,B} = C_{x^n+1} + E_{i,j}$ (že táto rovnosť platí plynie z vety 2.5) a v takom prípade platia rovnosti (2.1) a (2.2) odvodené v dôkaze vety 2.5.

Z toho, že $wt_{\oplus}(M_{\beta,B}) = 1$ navyše vieme, že $M_{\beta,B} = P + E_{i',j'}$, pre nejakú permutačnú maticu P a maticu $E_{i',j'}$, $i' \neq j'+1$. Preto existujú $l, m \in \{1,\ldots,n\}$ splňujúce

$$\beta b_{j+l} = b_{j+m}.$$

V indexoch prvkoch báze b_{j+k} budeme, rovnako ako v dôkaze vety 2.5, počítať $j+k \mod n$, $k \in \{1,\ldots,n\}$. Využitím rovnosti (2.1) dostaneme, že platí

$$b_{j+l} = \alpha^{l-1}\gamma$$
$$b_{j+m} = \alpha^{m-1}\gamma$$

pre $\gamma := b_{j+1}$. Dosadením do rovnice vyššie dostaneme

$$\beta\alpha^{l-1}\gamma = \alpha^{m-1}\gamma.$$

Keďže $\gamma \neq 0$ môžeme vydeliť danú rovnosť a po úprave dostaneme, že platí

$$\beta = \alpha^{m-l} =: \alpha^s,$$

kde $s \in \{-(n-1),\ldots,(n-1)\}$. Zrejme $s \neq 0$, inak by bolo $\beta = \alpha^0 = 1$, čo je spor z voľbou β (v takom prípade by matica reprezentujúca β reprezentovala 0 XOR operácií). Z toho plynie $l \neq m$.

Ostáva dokázať, že $-1 \leq s \leq 1$. Pre spor predpokladajme, že $s \geq 2$. Pozrime sa na to, ako násobenie prvkom β pôsobí na prvok $b_{j+(n-s+1)}$ bázy B. Z rovností (2.1) a (2.2) dostaneme vzťah

$$\beta b_{j+(n-s+1)} \overset{(2.1)}{=} \alpha^s\alpha^{n-s+1-1}\gamma = \alpha^n\gamma \overset{(2.2)}{=} \gamma + \alpha^t\gamma. \tag{2.3}$$

Opätovným použitím rovnosti (2.1) dostaneme výsledný vzťah

$$\beta b_{j+(n-s+1)} = \ldots = \gamma + \alpha^t\gamma \overset{(2.1)}{=} b_{j+1} + b_{j+t+1}. \tag{2.4}$$

Pretože $0 < t < n-1$ potom platí, že $b_{j+1} \neq b_{j+t+1}$. To teda znamená, že matica $M_{\beta,B}$ má v stĺpci $j+(n-s+1)$ pridanú jednotku.

Pre ďalší stĺpec matice rozlíšime dva prípady
1. prípad, pre $t < n-1$ platí

$$\beta b_{j+(n-s+2)} = \alpha^{n+1}\gamma = \alpha\gamma + \alpha^{t+1}\gamma \overset{(2.1)}{=} b_{j+2} + b_{j+t+2}.$$

2. prípad, pre $t = n-1$ platí

$$\beta b_{j+(n-s+2)} = \alpha^{n+1}\gamma = \alpha\gamma + \alpha^{(n-1)+1}\gamma \overset{(2.3)}{=} b_{j+2} + \beta b_{j+(n-s+1)} =$$
$$\overset{(2.4)}{=} b_{j+2} + b_{j+1} + b_{j+(n-1)+1} = b_{j+2} + b_{j+1} + b_j.$$

Taktiež ďalší stĺpec matice $M_{\beta,B}$ obsahuje aspoň jednu pridanú jednotku, čo je v spore s tým, že $wt_{\oplus}(M_{\beta,B}) = 1$. Preto určite platí $s < 2$.

Pre $-s \geq 2$ sa dokáže obdobne, ale uvažujeme β^{-1}, z čoho dostaneme $-s < 2$, teda $s > -2$. Ako už bolo vyššie spomenuté, zároveň platí $s \neq 0$. Preto platí $s \in \{-1, 1\}$.

Teda dostaneme hľadaný výsledok $\beta = \alpha^s = \alpha^{\pm 1}$.

□

Nakoniec budeme skúmať to, za akých podmienok je charakteristický polynóm matice (stupňa n s počtom XOR operácií 2) päťčlen stupňa n. Tento výsledok sa používa na hľadanie ľahkých prvkov pri väčších konečných telesách.

Veta 2.8. *Nech $A \in Mat_n(\mathbb{F}_2)$ je matica tvaru*

$$A = C_{x^n+1} + E_{i_1,j_1} + E_{i_2,j_2}$$

splňujúca nasledujúce podmienky

$$i_1 < j_1 \neq n;\ \ i_2 > j_2{+}1;\ \ i_1 \leq j_2;\ \ i_2 \leq j_1;\ \ j_1{-}(i_1{-}1) \neq n;\ \ n{-}(j_1{-}i_1) \neq i_2{-}j_2.$$

Potom charakteristický polynóm matice A je päťčlen stupňa n v tvare

$$\chi_A = \lambda^n + \lambda^{n+i_1-j_1+i_2-j_2-2} + \lambda^{n+i_1-j_1-1} + \lambda^{i_2-j_2-1} + 1.$$

Za takýchto podmienok platí $wt_{\oplus}(A) = 2$.

Dôkaz. Majme maticu $A = C_{x^n+1} + E_{i_1,j_1} + E_{i_2,j_2}$ splňujúcu podmienky v znení vety. Podmienky $i_1 < j_1 \neq n$ a $i_2 > j_2 + 1$ nám hovoria, že matica A má práve jeden pridaný nenulový prvok nad hlavnou diagonálou (v matici E_{i_1,j_1}) a druhý nenulový prvok pod hlavnou diagonálou (v matici E_{i_2,j_2}).

Chceme spočítať charakteristický polynóm matice A, teda z definície charakteristického polynómu počítame $\chi_A = \det(\lambda I_n - A)$. Determinant spočítame rozvojom podľa posledného stĺpca matice $\lambda I_n - A$. Pre lepší pohľad na výpočet sa pozrime na tvar danej matice

$$\lambda I_n - A = \begin{pmatrix} \lambda & & & & 1 \\ 1 & \lambda & & & 0 \\ & \ddots & \ddots & & \vdots \\ & & 1 & \lambda & 0 \\ & & & 1 & \lambda \end{pmatrix} + E_{i_1,j_1} + E_{i_2,j_2}.$$

Keďže platí, že $j_1, j_2, i_2 \neq n$ (plynie z podmienok $j_1 \neq n;\ i_2 \leq j_1;\ i_2 > j_2 + 1$) dostaneme, že

$$\chi_A = \det(S^{\lambda}_{n-1} + E_{i_1-1,j_1} + E_{i_2-1,j_2}) + \lambda \det(\lambda I_{n-1} + C_{x^{n-1}} + E_{i_1,j_1} + E_{i_2,j_2}).$$

Symbol S^{λ}_n bude označovať maticu stupňa n v tvare

$$S^{\lambda}_n := \begin{pmatrix} 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \\ & & & & 1 \end{pmatrix}.$$

Pre zjednodušenie výpočtu si označme

$$B := S^{\lambda}_{n-1} + E_{i_1-1,j_1} + E_{i_2-1,j_2}$$
$$C := \lambda I_{n-1} + C_{x^{n-1}} + E_{i_1,j_1} + E_{i_2,j_2}.$$

Počítame teda

$$\chi_A = \det(B) + \lambda \det(C).$$

Pre ďalší výpočet by sa nám hodilo, aby sme nenulový prvok nad hlavnou diagonálou v matici C, teda pridaný nenulový prvok z matice E_{i_1,j_1}, „dostali“ do pravého horného rohu matice. Matica C stupňa $n-1$ má tvar

$$C = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & \ddots & \ddots & & \\ & & 1 & \lambda & \\ & & & 1 & \lambda \end{pmatrix} + E_{i_1,j_1} + E_{i_2,j_2}.$$

To dosiahneme tým, že najprv $(n-1-j_1)$-krát budeme rozvíjať determinant podľa posledného stĺpca a potom budeme (i_1-1)-krát rozvíjať podľa prvého riadku matice C. Vďaka podmienke $i_2 \leq j_1$ vieme, že prvok pod diagonálou (teda nenulový prvok v matici E_{i_2,j_2}) nebude eliminovaný počas rozvíjania podľa posledného stĺpca a podmienka $i_1 \leq j_2$ nám zaručuje, že tento prvok nebude eliminovaný ani pri rozvoji podľa prvého riadku.

Dostaneme

$$\begin{aligned} \lambda \det(C) &= \lambda \lambda^{n-1-j_1} \lambda^{i_1-1} \det(\lambda I_{j_1-i_1+1} + C_{x^{j_1-i_1+1}+1} + E_{i_2-i_1+1,j_2-j_1+1}) \\ &= \lambda^{n-1-j_1+i_1} \det(\lambda I_{j_1-i_1+1} + C_{x^{j_1-i_1+1}+1} + E_{i_2-i_1+1,j_2-j_1+1}). \end{aligned}$$

Teda pridaný nenulový prvok nad hlavnou diagonálou je v pravom hornom rohu matice $\lambda I_{j_1-i_1+1} + C_{x^{j_1-i_1+1}+1} + E_{i_2-i_1+1,j_2-j_1+1}$. Pod diagonálou tiež ostal jeden pridaný nenulový prvok. Tvar tejto matice je

$$\lambda I_{j_1-i_1+1} + C_{x^{j_1-i_1+1}+1} + E_{i_2-i_1+1,j_2-j_1+1} = \begin{pmatrix} \lambda & & & & 1 \\ 1 & \lambda & & & 0 \\ & \ddots & \ddots & & \vdots \\ & & 1 & \lambda & 0 \\ & & & 1 & \lambda \end{pmatrix} + E_{i_2-i_1+1,j_2-j_1+1}.$$

Potrebujeme ešte spočítať determinant matice stupňa j_1-i_1+1. Pokračujeme rozvojom podľa posledného stĺpca. Dostaneme

$$\lambda \det(C) = \ldots = \lambda^{n-1-j_1+i_1}(\lambda^{j_1-i_1+1} + \det(S^{\lambda}_{j_1-i_1} + E_{i_2-i_1,j_2-j_1+1})).$$

Ostáva nám určiť determinant matice stupňa $j_1 - i_1$, u ktorej vieme, že má jeden nenulový prvok pod hlavnou diagonálou.

$$S^{\lambda}_{j_1-i_1} + E_{i_2-i_1,j_2-j_1+1} = \begin{pmatrix} 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \\ & & & & 1 \end{pmatrix} + E_{i_2-i_1,j_2-j_1+1}.$$

Tento prvok teraz chceme „dostať“ do ľavého dolného rohu tejto matice. Na hlavnej diagonále matice $S^{\lambda}_{j_1-i_1} + E_{i_2-i_1,j_2-j_1+1}$ sú jednotky, preto rozvoj podľa

posledného riadku alebo prvého stĺpca bude znamenať len zníženie dimenzie počítaného determinantu matice a násobenie príslušnej podmatice jednotkou. Najprv budeme rozvíjať $(j_1 - i_2)$-krát podľa posledného riadku. Dostaneme

$$\lambda \det(C) = \ldots = \lambda^{n-1-j_1+i_1}(\lambda^{j_1-i_1+1} + \det(S^{\lambda}_{i_2-i_1} + E_{i_2-i_1,j_2-j_1+1})).$$

Následne $(j_2 - j_1)$-krát rozvinieme podľa prvého stĺpca. Dostaneme

$$\lambda \det(C) = \ldots = \lambda^{n-1-j_1+i_1}(\lambda^{j_1-i_1+1} + \det(S^{\lambda}_{i_2-j_2} + E_{i_2-j_2,1})).$$

Pridaný nenulový prvok máme v ľavom dolnom rohu danej matice.

$$S^{\lambda}_{i_2-j_2} + E_{i_2-j_2,1} = \begin{pmatrix} 1 & \lambda & & & \\ 0 & 1 & \lambda & & \\ \vdots & & \ddots & \ddots & \\ 0 & & & 1 & \lambda \\ 1 & & & & 1 \end{pmatrix}.$$

Preto ostáva rozvinúť determinant matice $S^{\lambda}_{i_2-j_2} + E_{i_2-j_2,1}$ podľa prvého stĺpca. Dostaneme

$$\begin{aligned} \lambda \det(C) &= \ldots = \lambda^{n-1-j_1+i_1}(\lambda^{j_1-i_1+1} + (1 + \det(\lambda I_{i_2-j_2-1} + C_{x^{i_2-j_2-1}})) = \\ &= \lambda^{n-1-j_1+i_1}(\lambda^{j_1-i_1+1} + (1 + \lambda^{i_2-j_2-1})) = \\ &= \lambda^n + \lambda^{n+i_1-j_1+i_2-j_2-2} + \lambda^{n+i_1-j_1-1}. \end{aligned}$$

Dostávame teda trojčlen stupňa n. Posledný krok výpočtu determinantu je určený dolnou trojuholníkovou maticou stupňa $i_2 - j_2 - 1$, kde hlavná diagonála je zložená z prvkov λ a preto je jej determinant $\lambda^{i_2-j_2-1}$.

Potrebujeme ešte vypočítať $\det(B)$.

$$B = \begin{pmatrix} 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \\ & & & & 1 \end{pmatrix} + E_{i_1-1,j_1} + E_{i_2-1,j_2}.$$

Budeme postupovať obdobne. Našim cieľom je „dostať“ pridaný nenulový prvok pod hlavnou diagonálou do ľavého dolného rohu matice, teda do prvého stĺpca a posledného riadku. Preto determinant rozvinieme $(j_2 - 1)$-krát podľa prvého stĺpca. Vďaka podmienke $i_1 \leq j_2$ vieme, že predchádzajúci krok eliminuje pridaný nenulový prvok nad hlavnou diagonálou. Potom stačí rozvinúť determinant $(n - j_2 - (i_2 - j_2))$-krát podľa posledného stĺpca. Máme

$$\det(B) = \det(S^{\lambda}_{n-j_2} + E_{i_2-j_2,1}) = \det(S^{\lambda}_{i_2-j_2} + E_{i_2-j_2,1}).$$

Nakoniec rozvinieme determinant podľa prvého stĺpca matice

$$S^{\lambda}_{i_2-j_2} + E_{i_2-j_2,1} = \begin{pmatrix} 1 & \lambda & & & \\ 0 & 1 & \lambda & & \\ \vdots & & \ddots & \ddots & \\ 0 & & & 1 & \lambda \\ 1 & & & & 1 \end{pmatrix}$$

a dostaneme nasledujúci výsledok.

$$\det(B) = \ldots = \lambda^{i_2-j_2-1} + 1.$$

Konečne teda dostávame hľadaný výsledok

$$\chi_A = \det(B) + \lambda \det(C) = \lambda^n + \lambda^{n+i_1-j_1+i_2-j_2-2} + \lambda^{n+i_1-j_1-1} + \lambda^{i_2-j_2-1} + 1.$$

Fakt, že matica spĺňujca podmienky tejto vety má skutočne $wt_{\oplus}(A) = 2$ platí vďaka poznámke 1.26, pretože matica má tvar presne popísaný v tejto poznámke pre maticu s $wt_{\oplus} = 2$. V poznámke je uvedený prípad, kedy daná matica môže mať až 3 pridané nenulové prvky. Podmienky v znení tejto vety však tento prípad vylučujú a preto skutočne platí $wt_{\oplus}(A) = 2$.

Tým je tvrdenie dokázané.

□

Na záver tejto kapitoly uvedieme príklad matice, ktorá spĺňa podmienky predchádzajúcej vety a preto je jej charakteristický polynóm päťčlen.

Príklad 2.9. *Nech $A \in Mat_5(\mathbb{F}_2)$ je matica v tvare*

$$A = C_{x^5+1} + E_{2,4} + E_{4,2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Matica A spĺňuje všetky podmienky v znení vety 2.8 a preto podľa tejto vety platí

$$\begin{aligned} \chi_A &= \lambda^5 + \lambda^{5+2-4+4-2-2} + \lambda^{5+2-4-1} + \lambda^{4-2-1} + 1 = \\ &= \lambda^5 + \lambda^3 + \lambda^2 + \lambda + 1. \end{aligned}$$

Navyše aj minimálny polynóm matice A je práve polynóm $x^5 + x^3 + x^2 + x + 1$ (spočítané pomocou programu Wolfram Mathematica). Preto matica A reprezentuje násobenie prvkom α konečného telesa $\mathbb{F}_{2^5}$, ktorý má minimálny polynóm $m_\alpha = x^5 + x^3 + x^2 + x + 1$.

Záver

Cieľom mojej bakalárskej práce bolo naštudovanie a spracovanie témy rýchleho násobenia v konečných telesách, ktoré je užitočné pre implementáciu šifrovacích algoritmov v ľahkej kryptografii. Informácie o tejto téme som čerpal najmä z článku Beierle a kol. (2016), ale aj zo zdrojov uvedených v zozname použitej literatúry. Zaujímavé tvrdenia z uvedeného článku som spracoval tak, aby boli ľahšie pochopiteľné a v danej problematike sa dokázal zorientovať aj čitateľ, ktorý sa s danou témou ešte nestretol. Uviedol som niektoré pomocné tvrdenia z lineárnej algebry a konečných telies (niektoré aj s dôkazom, iné s informáciou, kde dôkaz hľadať), ktoré boli potrebné pre dôkaz hlavných tvrdení zo spomínaného článku.

V práci som uviedol niekoľko príkladov pre jednoduchšie pochopenie danej témy. Už v úvode som uviedol, na čo sa spracovávaná téma dá využiť aj s konkrétnymi príkladmi z praxe. To čitateľovi tejto práce umožní širší pohľad na skúmaný problém, a aj to, kde sa s ním dá stretnúť. V prvej kapitole sú uvedené príklady doplňujúce niektoré tvrdenia tak, aby boli jasne pochopiteľné. V závere druhej kapitoly je uvedený príklad matice, ktorá sa dá implementovať len s dvoma XOR operáciami.

Prínos tejto práce vidím najmä v komplexnejšom poňatí a podrobnejšom vysvetlení celého problému. To znamená, že čitateľ prácu číta od príkladov využitia z praxe, uvedených v úvode, cez jednoduhšie pojmy v prvej kapitole, s ktorými sa čitateľ už zrejme stretol, ale je vhodné ich pripomenutie. Následne sa má čitateľ možnosť zoznámiť s problematikou počtu XOR operácií potrebných na implemetáciu prvku konečného telesa, na ktorú nadväzuje druhá kapitola, ktorá dáva jasné výsledky, ako voliť prvky konečného telesa, ktoré sa dajú implementovať s malým počtom XOR operácií.

Na záver ešte stručne uveďme príklad praktického využitia voľby prvkov konečného telesa, ktoré sa dajú implementovať s minimom XOR operácií. Ide o aplikáciu v MDS maticiach, ktoré využívajú viaceré šifrovacie algoritmi. Pripomeňme, že MDS (Maximum Distance Separable) matica je matica generujúca MDS kód, čo je kód s maximálnou možnou Hammingovou vzdialenosťou. V nami študovanom článku Beierle a kol. (2016) je uvedená konštrukcia cyklických MDS matíc, ktoré sa dajú efektívne implementovať. Táto konštrukcia je postavená tak, aby sa pri násobení danou maticou minimalizoval počet násobení s fixným prvkom konečného telesa, ktorého mocniny sú prvkami danej MDS matice. Voľba MDS matice ako cyklickej matice zase umožňuje rýchle rozhodnutie, či je daná matica MDS alebo nie. Daná konštrukcia matice vychádza z matice s prvkami z podgrupy telesa zlomkov polynomiálneho okruhu $\mathbb{F}_2[x]$. Z vlastnosti MDS matíc, že matica je MDS práve vtedy, keď je každá jej štvorcová podmatica regulárna, sa zostaví zoznam podmienok na danú maticu, za ktorých je MDS. Tento zoznam tvoria práve ireducibilné prvky charakteristických polynómov všetkých štvorcových podmatíc danej matice. Z vlastnosti MDS matice, ktorú sme vyššie spomenuli, je zrejmé, že matica je MDS práve vtedy, keď všetky polynómy v danom zozname sú nenulové, inak by bola nejaká štvorcová podmatica singulárna a potom by daná matica nebola MDS. Do takto pripravenej matice chceme za prvok x dosadiť prvok konečného telesa, ktorý sa dá implementovať s minimom XOR operácií. Stačí zvoliť taký prvok, ktorý nie je koreňom žiadneho polynómu v

uvedenom zozname a potom bude matica skutočne MDS a implementovateľná s minimom XOR operácií. Na určenie, či je daný prvok konečného telesa koreňom nejakého z týchto polynómov stačí overiť, že minimálny polynóm tohto prvku nie je v danom zozname polynómov, pretože je to tiež ireducibilný polynóm.

Zoznam použitej literatúry

Barto, L. a Tůma, J. (2014). Lineární algebra. http://www.karlin.mff.cuni.cz/~tuma/LinAlg14-15/skripta.pdf.

Barto, L. a Tůma, J. (2017). Konečná tělesa. http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf.

Beierle, C., Kranz, T. a Leander, G. (2016). Lightweight Multiplication in GF(2^n) with Applications to MDS Matrices. Cryptology ePrint Archive, Report 2016/119. https://eprint.iacr.org/2016/119.

Bečvář, J. (2005). *Lineární algebra*. Tretie vydanie. Matfyzpress, Praha. ISBN 80-86732-57-6.

Cole, P. H. a Ranasinghe, D. C. (2008). *Networked RFID Systems and Lightweight Cryptography*. Prvé vydanie. Springer-Verlag Berlin Heidelberg, Adelaide. ISBN 978-3-540-71640-2.

Conrad, K. The minimal polynomial and some applications. http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/minpolyandappns.pdf.

CryptoLUX (2016). Lightweight Cryptography. https://www.cryptolux.org/index.php/Lightweight_Cryptography.

Dummit, D. S. a Foote, R. M. (2004). *Abstract Algebra*. Tretie vydanie. John Wiley, Hoboken. ISBN 0-471-43334-9.

Hoffman, K. a Kunze, R. (1971). *LINEAR ALGEBRA*. Druhé vydanie. Prentice-Hall, Englewood Cliffs. ISBN 978-0135367971.

Journal, R. (2003). Hitachi Unveils Smallest RFID Chip. RFID Journal. http://www.rfidjournal.com/articles/view?337.

Mouha, N. (2015). The Design Space of Lightweight Cryptography. Cryptology ePrint Archive, Report 2015/303. https://eprint.iacr.org/2015/303.

Sim, S. M., Khoo, K., Oggier, F. a Peyrin, T. (2015). Lightweight MDS Involution Matrices. Cryptology ePrint Archive, Report 2015/258. https://eprint.iacr.org/2015/258.

Swedberg, C. (2017). Researchers Develop Microscopic RFID Chip to Embed in Human Cells. RFID Journal. http://www.rfidjournal.com/articles/view?16498/.

Wardlaw, W. P. (1994). Matrix representation of finite fields. https://www.maa.org/sites/default/files/Wardlaw47052.pdf.

Zlatoš, P. (2011). *Lineárna algebra a geometria*. Prvé vydanie. Marenčin PT, Bratislava. ISBN 978-80-8114-111-9.