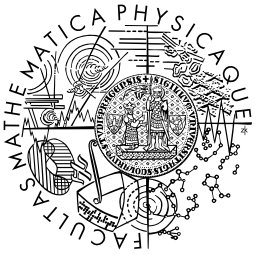

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁRSKA PRÁCA

Marek Marko

Kryptosystémy založené na kódoch s hodnostnou metrikou

Katedra algebry

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

Študijný program: Matematika

Študijný obor: Matematika pre informačné technológie

Praha 2021

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne a výhradne s použitím citovaných prameňov, literatúry a ďalších odborných zdrojov. Táto práca nebola využitá na získanie iného alebo rovnakého titulu.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Zb., autorského zákona v platnom znení, najmä skutočnosť, že Univerzita Karlova má právo na uzavretie licenčnej zmluvy o použití tejto práce ako školského diela podľa §60 ods. 1 autorského zákona.

V ..... dňa ....

Podpis autora

Touto cestou by som sa chcel poďakovať vedúcemu mojej bakalárskej práce doc. Mgr. et Mgr. Janovi Žemličkovi, Ph.D. za ochotu, užitočné rady a odbornú pomoc poskytnuté pri jej písaní.

Názov práce: Kryptosystémy založené na kódoch s hodnostnou metrikou

Autor: Marek Marko

Katedra: Katedra algebry

Vedúcí bakalárskej práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., katedra algebry

Abstrakt: Jedným z cieľov práce je čitateľovi zrozumiteľne popísať využitie hodnosti prvku a ňou indukovanej metriky v lineárnych kódoch nad konečnými telesami. Dôležitou súčasťou je vysvetlenie efektívneho dekódovacieho algoritmu danej triedy samoopravných kódov, kedy nedochádza k časovo náročnému prehľadávaniu hrubou silou. Práve tento algoritmus využijeme v kryptografickom systémé založenom na kódoch s hodnostnou metrikou, ktorým sa zaoberá ďalšia časť práce. Okrem samotnej schémy kryptosystému je dôraz kladený na detailné ilustrovanie možného štrukturálneho útoku naň. Porozumenie danému útoku zohráva kľúčovú úlohu pre popísanie spôsobu obrany voči nemu.

Kľúčové slová: hodnostná metrika, lineárne samoopravné kódy, kryptosystém

Title: Cryptosystems based on codes with rank metrics

Author: Marek Marko

Department: Department of Algebra

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

Abstract: The first part of this paper explains the uses of the element's rank and the metric induced by it in linear error-correcting codes over finite fields. Describing the effective decoding algorithm of rank-metric codes without the use of exhaustive search is essential. This algorithm is applied in cryptographic systems based on codes with rank metric presented in the next chapter. Apart from the scheme of cryptosystem, we focus on the detailed illustration of a possible structural attack. Comprehension of the attack will be significant in order to show some methods how to withstand it.

Keywords: rank metric, linear error-correcting codes, cryptosystem

Obsah

Úvod

Potreba komunikácie a dorozumievania sa je nepochybne stará ako ľudstvo samo. Rovnako tak už prastaré civilizácie chápali, aké dôležité je niekedy jej utajenie. Najdôležitejšie a zároveň najnebezpečnejšie tajomstvá boli tie vojnové. Keby nepriateľ poznal vopred stratégiu, akú sa chystáme použiť, vedel by sa na ňu adekvátne pripraviť a nám by nebola nič platná. Preto zapísanie stratégie zrozumiteľnou rečou malo potenciál zmariť všetky šance na úspech. To bol jeden z hlavných dôvodov začiatku kryptografie. Dnes je potreba utajenia a zabezpečenia komunikácie ešte omnoho dôležitejšia a to i v životoch bežných ľudí. V súčasnosti, keď už namiesto návštevy banky alebo úradov, stačí pár kliknutí, sú nároky na bezpečnosť neporovnateľné. Samotné šifrovanie obsahu správy je vyžadované na úrovni samozrejmosti.

Obsahom tejto práce nie je skúmanie aspektov kryptografie a zabezpečovania komunikácie, ale popísanie možného spôsobu šifrovania. Náš cieľ v tejto práci sa dá rozčleniť na tri časti. Najprv zdôraznime, že vo všetkých častiach budeme pracovať s dvomi konečnými telesami, kde jedno bude rozširovať to druhé. S výhodou využijeme, že väčšie teleso má nad menším štruktúru vektorového priestoru. Hneď na začiatok prvej časti zavedieme hodnosť prvku väčšieho telesa nad menším a tejto hodnosti využijeme následne ako metriky v lineárnych kódoch. Špeciálne sa zameriame na vybudovanie potrebnej teórie o triede kódov s hodnostnou metrikou definovanej Ernstom M. Gabidulinom v roku 1985, ktoré spadajú do triedy MDS (Maximum Distance Separable) kódov. Okrem vlastností Gabidulinovych kódov sa zameriame aj na popísanie algoritmu opravy chýb využívajúceho lineárnej algebry nad oboma telesami.

V druhej časti práce predstavíme kryptografické systémy na týchto kódoch založené, čiže spôsoby šifrovania a dešifrovania správ využívajúce zavedenej teórie. Základná myšlienka je prevzatá z McElieceovej schémy asymetrického kryptosystému z roku 1978, ktorá v procese šifrovania využíva práve samoopravné kódy. Prvý kryptosystém založený na kódoch hodnostnej metriky publikovaný pánmi Gabidulinom, Paramonovom a Tretjakovom v roku 1991 nesie označenie GPT kryptosystém. Okrem schémy GPT kryptosystému popíšeme i schému modifikujúcu Niederreiterov asymetrický kryptosystém. Zároveň overíme správnosť daných schém kryptosystémov, teda či dešifrovaním zašifrovanej správy dostaneme pôvodnú správu.

Na bezpečnosť GPT kryptosystému sa pozrieme v poslednej časti práce. V prvom kroku popíšeme potenciálnu slabinu schémy, ktorej využijeme v ďalšom kroku pri formulovaní Overbeckovho štrukturálneho útoku z roku 2005. Cieľom tohto útoku je získať alternatívny súkromný kľúč zo známeho verejného kľúča, čiže úplne prelomiť bezpečnosť šifrovania. Útok detailne rozoberieme od idey cez postup prevedenia až po ilustráciu na príkladoch. V poslednom kroku zhrnieme nejaké známe spôsoby obrany voči tomuto útoku.

1. Kódy najvzdialenejšej hodnosti

1.1 Kódy hodnostnej metriky

Dovoľujeme si začať zavedením značenia. Buď q prvočíslo a $m \in \mathbb{N}$, potom konečné teleso o q^m prvkoch značíme $\mathbb{F}_{q^m}$ a má štruktúru vektorového priestoru nad $\mathbb{F}_q$. Ďalej hodnosť matice $A \in \mathbb{F}_{q^m}^{n\times k}$, kde $n, k \in \mathbb{N}$, značíme $\mathrm{rank}(A)$ a dimenziu vektorového priestoru $\mathbb{V}$ značíme $\dim(\mathbb{V})$. Prvky kanonickej bázy priestoru $\mathbb{V}$ budeme značiť $\delta_i = (\delta_{ij})_{j=1}^{\dim(\mathbb{V})}$, kde $\delta_{ii} = 1$ a $\delta_{ij} = 0$ pre všetky $j \neq i$.

V celej tejto časti budeme spracovávať a rozširovať druhú kapitolu z článku Tan a kol. (2018).

Definícia 1. *Nech $k, n \in \mathbb{N}$ a $(\alpha_1, \alpha_2, \ldots, \alpha_m)$ je báza $\mathbb{F}_{q^m}$ nad $\mathbb{F}_q$. Pre prvok $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}^n$ a $1 \leq i \leq n$ môžeme písať $a_i = \sum_{j=1}^m a_{ji} \cdot \alpha_j$, kde $a_{ji} \in \mathbb{F}_q$. Potom* hodnosť prvku $\mathbf{a}$ nad $\mathbb{F}_q$*, ktorú budeme značiť* $\mathrm{rk}(\mathbf{a})$*, definujeme ako hodnosť matice $A = (a_{ij}) \in \mathbb{F}_q^{m\times n}$, čiže $\mathrm{rk}(\mathbf{a}) = \mathrm{rank}(A)$. Ďalej pre maticu $M = (M_1|\ldots|M_k) \in \mathbb{F}_{q^m}^{n\times k}$ definujeme* stĺpcovú hodnosť matice M nad $\mathbb{F}_q$ *ako* $\mathrm{rank}_q^{|}(M) = \dim(\mathrm{LO}_{\mathbb{F}_q}\{M_1, \ldots, M_k\})$*, teda ako najväčší možný počet stĺpcov matice M, ktoré sú lineárne nezávislé pri vyjadrení nad telesom $\mathbb{F}_q$.*

Poznámka. Nech $k, n \in \mathbb{N}$ a $M \in \mathbb{F}_{q^m}^{n\times k}$. Potom budeme rozlišovať dve hodnosti matice M, a to „klasickú“ hodnosť $\mathrm{rank}(M)$ nad $\mathbb{F}_{q^m}$ a stĺpcovú hodnosť $\mathrm{rank}_q^{|}(M)$ nad $\mathbb{F}_q$.

Teraz by sme si mohli položiť otázku, aký má vzťah hodnosť prvku vektorového priestoru $\mathbb{F}_{q^m}^n$ s dimenziou priestoru generovaného zložkami tohto prvku. Okrem lepšieho porozumenia hodnosti, sa nám tento vzťah vyplatí poznať i v neskorších tvrdeniach. Odpoveď na túto otázku nám poskytne špeciálny pripad nasledujúceho tvrdenia.

Tvrdenie 2. *Nech $k, l \in \mathbb{N}$, $A = (a_1, \ldots, a_k)$ je lineárne nezávislá postupnosť prvkov nad $\mathbb{F}_q$ a $b_1, \ldots, b_l \in \mathrm{LO}(A)$. Potom pre maticu $B = ([b_1]_A|\ldots|[b_l]_A)$ platí $\mathrm{rank}(B) = \dim(\mathrm{LO}(b_1, \ldots, b_l))$, kde $[b_i]_A$ značí stĺpcový vektor súradníc prvku b_i v báze A.*

Dôkaz. *Označme $\mathbb{U} = \mathrm{LO}(b_1, \ldots, b_l)$ a $\mathbb{V} = \mathrm{LO}([b_1]_A, \ldots, [b_l]_A)$. Definujme zobrazenie $\varphi : \mathbb{U} \to \mathbb{V}$ predpisom $\varphi(x) = [x]_A$ pre prvky $x \in \mathbb{U}$. Zobrazenie je zrejme dobre definované, prosté i na, pretože z lineárnej algebry vieme, že vyjadrenie prvku v konkrétnej báze je jednoznačne určené. Zároveň z lineárnej algebry vieme, že pre ľubovoľné $x, y \in \mathbb{U}, t \in \mathbb{F}_q : [x + y]_A = [x]_A + [y]_A, [t \cdot x]_A = t \cdot [x]_A$, takže φ je bijektívny homomorfizmus, a teda izomorfizmus. Na záver už len pripomeňme ďalší poznatok z lineárnej algebry, a to, že obraz ľubovoľnej bázy priestoru $\mathbb{U}$ je pri izomorfizme bázou priestoru $\mathbb{V}$. Odtiaľto teda plynie požadovaná rovnosť $\dim(\mathbb{U}) = \dim(\mathbb{V}) = \mathrm{rank}(B)$.*

□

Dôsledok. Nech $n \in \mathbb{N}$ a $\mathbf{a} \in \mathbb{F}_{q^m}^n$. Potom $\mathrm{rk}(\mathbf{a}) = \dim(\mathrm{LO}_{\mathbb{F}_q}(\mathbf{a}))$, čiže hodnosť prvku nie je závislá na zvolenej báze $\mathbb{F}_{q^m}$ nad $\mathbb{F}_q$, ale je určená jednoznačne.

Než pokročíme ďalej, je dôležité si pripomenúť, čo si predstavíme pod pojmom metrika. Majme množinu $\mathbf{X}$. Zobrazenie $\rho : \mathbf{X} \times \mathbf{X} \to \langle 0, \infty)$ nazveme metrikou, ak platí:

1. $\forall x, y \in \mathbf{X} : \rho(x, y) = 0 \iff x = y$,
2. $\forall x, y \in \mathbf{X} : \rho(x, y) = \rho(y, x)$,
3. $\forall x, y, z \in \mathbf{X} : \rho(x, z) \leq \rho(x, y) + \rho(y, z)$.

Tvrdenie 3. *Nech $n \in \mathbb{N}$. Zobrazenie priraďujúce dvojici prvkov $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^m}^n$ hodnotu $\mathrm{rk}(\mathbf{a} - \mathbf{b})$ je metrikou na $\mathbb{F}_{q^m}^n$.*

Dôkaz. Zvoľme $\mathbf{a} = (a_1, \ldots, a_n), \mathbf{b} = (b_1, \ldots, b_n), \mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_{q^m}^n$ a označme $A = (a_{ij}), B = (b_{ij}), C = (c_{ij})$. Overíme podmienky z pripomenutia nad tvrdením:

1. $\mathrm{rk}(\mathbf{a} - \mathbf{b}) \geq 0 \iff \mathrm{rank}(A - B) \geq 0$, *čo platí priamo z definície hodnosti matice. Teraz nech* $\mathrm{rk}(\mathbf{a} - \mathbf{b}) = 0$. *Teda* $\mathrm{rank}(A - B) = 0$, *z čoho plynie* $A - B = 0_{m \times n}$. *Takže* $A = B \implies \mathbf{a} = \mathbf{b}$.

2. $\mathrm{rk}(\mathbf{a}-\mathbf{b}) = \mathrm{rank}(A-B) = \mathrm{rank}((-1)(A-B)) = \mathrm{rank}(B-A) = \mathrm{rk}(\mathbf{b}-\mathbf{a})$, *kde sme využili, že elementárne úpravy nemenia hodnosť matice.*

3. *Najprv ukážeme, že platí* $\mathrm{rank}(A+B) \leq \mathrm{rank}(A)+\mathrm{rank}(B)$. *Pretože priestor* $\mathrm{Im}(A+B)$ *je obsiahnutý v* $\mathrm{Im}(A) + \mathrm{Im}(B)$, *tak podľa vety o dimenzii súčtu a prieniku z lineárnej algebry máme:*

$$\begin{aligned} \mathrm{rank}(A + B) &= \dim(\mathrm{Im}(A + B)) \leq \dim(\mathrm{Im}(A) + \mathrm{Im}(B)) \\ &= \dim(\mathrm{Im}(A)) + \dim(\mathrm{Im}(B)) - \dim(\mathrm{Im}(A) \cap \mathrm{Im}(B)) \\ &= \mathrm{rank}(A) + \mathrm{rank}(B) - \dim(\mathrm{Im}(A) \cap \mathrm{Im}(B)). \\ \implies \mathrm{rk}(\mathbf{a} - \mathbf{c}) &= \mathrm{rank}(A - C) = \mathrm{rank}(A - B + B - C) \\ &\leq \mathrm{rank}(A - B) + \mathrm{rank}(B - C) = \mathrm{rk}(\mathbf{a} - \mathbf{b}) + \mathrm{rk}(\mathbf{b} - \mathbf{c}). \end{aligned}$$

Tým sme dokázali tvrdenie.

□

V ďalšom kroku je pre nás nevyhnutné si osvojiť základné pojmy a značenia z teórie kódov.

Definícia 4. *Nech $n, k \in \mathbb{N}$.* Lineárny kód $\mathcal{C}$ dĺžky n a dimenzie k *je podpriestor vektorového priestoru $\mathbb{F}_{q^m}^n$ nad telesom $\mathbb{F}_{q^m}$ dimenzie k a budeme ho značiť $[n, k]_{q^m}$-kód.*
Generujúca matica $[n, k]_{q^m}$*-kódu $\mathcal{C}$ je matica $G \in \mathbb{F}_{q^m}^{k \times n}$ hodnosti k, ktorej riadkové vektory generujú všetky prvky nazývané kódové slová ako $\mathcal{C} = \{\eta \cdot G \mid \eta \in \mathbb{F}_{q^m}^k\}$.*
Kontrolná matica $[n, k]_{q^m}$*-kódu $\mathcal{C}$ je matica $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ hodnosti $n-k$, pre ktorú platí $G \cdot H^\top = 0_{k \times (n-k)}$, kde G je generujúca matica kódu $\mathcal{C}$.*
Duálny kód *kódu $\mathcal{C}$ je $\mathcal{C}^\perp = \mathrm{Im}(H^\top)$, kde H je kontrolná matica kódu $\mathcal{C}$.*

Pretože každý prvok $[n, k]_{q^m}$-kódu $\mathcal{C}$ vieme vyjadriť ako $\mathbf{x} = \eta \cdot G$ pre $\eta \in \mathbb{F}_{q^m}^k$, tak potom platí $\mathbf{x} \cdot H^\top = \eta \cdot G \cdot H^\top = \eta \cdot 0_{k \times (n-k)} = \mathbf{o}$. Ďalej vieme pre každý $[n, k]_{q^m}$-kód $\mathcal{C}$ až na permutačnú ekvivalenciu nájsť generujúcu maticu $G \in \mathbb{F}_{q^m}^{k \times n}$ v štandardnom tvare, tj. $G = \begin{bmatrix} I_k & X \end{bmatrix}$, kde I_k je jednotková matica a $X \in \mathbb{F}_{q^m}^{k \times (n-k)}$.

Definícia 5. *Povieme, že* $[n,k]_{q^m}$*-kód* $\mathcal{C}$ *nad* $\mathbb{F}_{q^m}$ *je* kód hodnostnej metriky*, ak ako vzdialenosť dvoch kódových slov* $\mathbf{x},\mathbf{y}\in\mathcal{C}$ *berieme* $\mathrm{rk}(\mathbf{x}-\mathbf{y})$*. Ďalej definujeme* minimálnu vzdialenosť *kódu* $\mathcal{C}$ *ako* $d(\mathcal{C})=\min\{\mathrm{rk}(\mathbf{x}-\mathbf{y})\mid\mathbf{x},\mathbf{y}\in\ \mathcal{C};\mathbf{x}\neq\mathbf{y}\}$.

Hlavným cieľom teórie kódov je nájsť najväčší možný kód pre danú minimálnu vzdialenosť kódových slov. Základným a všeobecne používaným odhadom v teórii kódov pri Hammingovej vzdialenosti je takzvaná Singletonova hranica, ktorá udáva najväčší možný počet kódových slov kódu $\mathcal{C}$ dĺžky n a minimálnej vzdialenosti d. Presnejšie sformulovaná Singletonova hranica je, že pre každý $[n,k]_{q^m}$-kód $\mathcal{C}$ s Hammingovou vzdialenosťou platí $d_{\mathcal{H}}(\mathcal{C})\leq n-k+1$, kde $d_{\mathcal{H}}(\mathcal{C})$ je minimálna Hammingova vzdialenosť tohto kódu. Viac o samoopravných kódoch sa môžete dočítať napríklad v skriptách A. Drápala. Teraz je pre nás nevyhnutné zaviesť podobný odhad pre kódy hodnostnej metriky.

Tvrdenie 6 (Kvázi-Singletonova hranica)**.** *Nech* $n,k\in\mathbb{N},n\leq m$ *a majme* $[n,k]_{q^m}$*-kód* $\mathcal{C}$ *nad* $\mathbb{F}_{q^m}$ *s hodnostnou metrikou. Potom* $d(\mathcal{C})\leq d_{\mathcal{H}}(\mathcal{C})\leq n-k+1$.

Dôkaz. Nájdime nejakú bázu β *priestoru* $\mathcal{C}$*. Zvoľme prvky* $\mathbf{a}=(a_1,\ldots,a_n)$, $\mathbf{b}=(b_1,\ldots,b_n)\in\mathcal{C}$*. Pripomeňme, že Hammingova vzdialenosť dvoch kódových slov je počet ich rozdielnych súradníc. Inými slovami, Hammingova vzdialenosť* $\mathbf{a}$ *a* $\mathbf{b}$ *je počet nenulových zložiek prvku* $\mathbf{a}-\mathbf{b}=(a_1-b_1,\ldots,a_n-b_n)$*. Ďalej vieme, že hodnostná vzdialenosť týchto dvoch prvkov je definovaná ako* $\mathrm{rk}(\mathbf{a}-\mathbf{b})=\mathrm{rank}\left(([a_1-b_1]_\beta|\ldots|[a_n-b_n]_\beta)\right)$*, teda dimenzia priestoru generovaného zložkami ich rozdielu. Odtiaľto však plynie, že* $d(\mathcal{C})\leq d_{\mathcal{H}}(\mathcal{C})$*, pretože dimenzia priestoru generovaného týmto rozdielom je rovná počtu lineárne nezávislých zložiek* $\mathbf{a}-\mathbf{b}$*, čo nemôže byť väčšie než počet jeho nenulových zložiek.*

Tvrdenie teda plynie zo Singletonovej hranice pre kódy s Hammingovou vzdialenosťou, pretože $d(\mathcal{C})\leq d_{\mathcal{H}}(\mathcal{C})\leq n-k+1$.

□

Dôsledok. Lineárny $[n,k]_{q^m}$-kód $\mathcal{C}$ s hodnostnou metrikou, pre ktorý nastáva rovnosť $d(\mathcal{C})=n-k+1$, patrí do skupiny MDS (Maximum Distance Separable) kódov.

1.2 Kódy najvzdialenejšej hodnosti

V minulom tvrdení sme si dokázali horný odhad minimálnej vzdialenosti $[n,k]_{q^m}$-kódu s hodnostnou metrikou. Teraz sa zameriame na triedu kódov hodnostnej metriky, pre ktorú nastáva rovnosť v tomto odhade. Ďalej budeme pokračovať v spracovávaní a dopĺňaní druhej a tretej kapitoly článku Tan a kol. (2018).

Definícia 7. *Povieme, že kód hodnostnej metriky* $\mathcal{C}$ *je* kódom najvzdialenejšej hodnosti (KNH)*, ak* $d(\mathcal{C})=n-\dim(\mathcal{C})+1$.

Takže $[n,k]_{q^m}$-kód $\mathcal{C}$ je KNH, ak všetky navzájom rôzne kódové slová $\mathcal{C}$ majú vzájomnú vzdialenosť aspoň $n-k+1$, tj. $\forall\mathbf{x},\mathbf{y}\in\mathcal{C},\mathbf{x}\neq\mathbf{y}:\mathrm{rk}(\mathbf{x}-\mathbf{y})\geq n-k+1$. To ale znamená, že hodnosť všetkých kódových slov kódu najvzdialenejšej hodnosti je aspoň $n-k+1$. Vďaka tejto vlastnosti patria KNH do skupiny kódov MDS.

Lemma 8. *Nech* $r \in \mathbb{N}, \mathbf{a} \in \mathbb{F}_{q^m}^n$ *také, že* $\mathrm{rk}(\mathbf{a}) = r$. *Potom existujú* $\tilde{\mathbf{a}} \in \mathbb{F}_{q^m}^r$ *a* $U \in \mathbb{F}_q^{r \times n}, \mathrm{rank}(U) = r$ *spĺňujúce* $\mathbf{a} = \tilde{\mathbf{a}} \cdot U$.

Dôkaz. *Označme* $\mathbf{a} = (a_1, \ldots, a_n)$. *Podľa dôsledku tvrdenia 2 pre dimenziu platí* $\dim(\mathrm{LO}_{\mathbb{F}_q}(a_1, \ldots, a_n)) = \mathrm{rk}(\mathbf{a}) = r$ *a môžeme nájsť bázu* $\tilde{\mathbf{a}} = (\tilde{a}_1, \ldots, \tilde{a}_r)$ *tohto priestoru nad* $\mathbb{F}_q$. *Potom zrejme* $\tilde{\mathbf{a}} \in \mathbb{F}_{q^m}^r$. *Položme* $U = ([a_1]_{\tilde{\mathbf{a}}} | \ldots | [a_n]_{\tilde{\mathbf{a}}})$ *maticu typu* $r \times n$, *teda* $U \in \mathbb{F}_q^{r \times n}$. *Z tvrdenia 2 dostávame* $\mathrm{rank}(U) = \dim(\mathrm{LO}_{\mathbb{F}_q}(\tilde{\mathbf{a}})) = r$. *Z voľby* $\tilde{\mathbf{a}}$ *a* U *priamo plynie* $\mathbf{a} = \tilde{\mathbf{a}} \cdot U$.

□

Lemma 9. *Nech* $\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^m}^n$. *Potom* $\mathrm{rk}(\mathbf{u} + \mathbf{v}) \geq \mathrm{rk}(\mathbf{u}) - \mathrm{rk}(\mathbf{v})$.

Dôkaz. *Pre ľubovoľne* $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^m}^n$ *platí* $\mathrm{rk}(\mathbf{a}-\mathbf{b}) \leq \mathrm{rk}(\mathbf{a}) + \mathrm{rk}(\mathbf{b})$, *pretože hodnosť súčtu matíc nie je väčšia než súčet hodností matíc a* $\mathrm{rk}(\mathbf{b}) = \mathrm{rk}(-\mathbf{b})$. *Položme* $\mathbf{a} = \mathbf{u}+\mathbf{v}$ *a* $\mathbf{b} = \mathbf{v}$. *Potom* $\mathrm{rk}(\mathbf{u}) \leq \mathrm{rk}(\mathbf{u}+\mathbf{v}) + \mathrm{rk}(\mathbf{v})$. *Odčítaním* $\mathrm{rk}(\mathbf{v})$ *dostávame nerovnosť.*

□

Tvrdenie 10. *Nech* $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ *je kontrolná matica* $[n, k]_{q^m}$*-kódu* $\mathcal{C}$ *s minimálnou vzdialenosťou aspoň* d. *Označme* $\mathbf{s} = \mathbf{e} \cdot H^\top$, *kde* $\mathbf{e} \in \mathbb{F}_{q^m}^n, \mathrm{rk}(\mathbf{e}) \leq r$. *Potom:*

1. *Množina všetkých riešení* $\mathbf{x}$ *spĺňujúcich* $\mathbf{s} = \mathbf{x} \cdot H^\top$ *je* $\{\mathbf{w} + \mathbf{e} \mid \mathbf{w} \in \mathcal{C}\}$.
2. *Ak* $\mathbf{w} \in \mathcal{C} \setminus \{\mathbf{o}\}$, *potom* $\mathrm{rk}(\mathbf{w} + \mathbf{e}) \geq d - r$.

Dôkaz.

1. *Zrejme* $\mathbf{s} = \mathbf{x} \cdot H^\top$ *platí práve vtedy, keď platí* $\mathbf{e} \cdot H^\top = \mathbf{x} \cdot H^\top$, *čo nastane práve, keď* $(\mathbf{x} - \mathbf{e}) \cdot H^\top = \mathbf{o}$. *Vieme že pre každé kódové slovo* $\mathbf{y} \in \mathcal{C}$ *platí* $\mathbf{y} \cdot H^\top = \mathbf{o}$, *takže dostávame* $\mathbf{x} - \mathbf{e} \in \mathcal{C}$. *Odtiaľto plynie, že* $\mathbf{x}$ *je riešením* $\mathbf{s} = \mathbf{x} \cdot H^\top$ *práve vtedy, keď* $\mathbf{x} = \mathbf{e} + \mathbf{w}$ *pre nejaké* $\mathbf{w} \in \mathcal{C}$.
2. *Z lemmy 9 dostávame* $\mathrm{rk}(\mathbf{w} + \mathbf{e}) \geq \mathrm{rk}(\mathbf{w}) - \mathrm{rk}(\mathbf{e}) = \mathrm{rk}(\mathbf{w}) - r \geq d - r$, *pretože* $\mathbf{w} \neq \mathbf{o}$.

Tým sme dokázali obe časti tvrdenia.

□

Konečne sme už oboznámení so základnou terminológiou lineárnych kódov, špeciálne KNH. Teraz sa môžeme ešte pozrieť na podmienky, kedy je lineárny kód kódom najvzdialenejšej hodnosti a aké má vlastnosti. Dôkaz nasledujúceho technického tvrdenia vynecháme.

Tvrdenie 11 (Gabidulin, 1985, Veta 2)**.** *Nech* k,$n \in \mathbb{N}$ *a* $G \in \mathbb{F}_{q^m}^{k \times n}$ *je generujúca matica* $[n, k]_{q^m}$*-kódu* $\mathcal{C}$. *Potom* $\mathcal{C}$ *je KNH práve vtedy, keď* $\mathrm{rank}(V \cdot G^\top) = k$ *pre všetky matice* $V \in \mathbb{F}_q^{k \times n}$ *hodnosti* k.

Veta 12 (Nutné podmienky pre KNH)**.** *Nech* $n, k \in \mathbb{N}, 2k < n \leq m$ *a majme maticu* $G = \begin{bmatrix} I_k & X \end{bmatrix} \in \mathbb{F}_{q^m}^{k \times n}$ *generujúcu* $[n, k]_{q^m}$*-kód* $\mathcal{C}$, *kde* $X = (x_{ij}) \in \mathbb{F}_{q^m}^{k \times (n-k)}$. *Označme* $d = n - k + 1$. *Ak je* $\mathcal{C}$ *KNH, tak potom:*

1. $[n - k, k]_{q^m}$*-kód* $\tilde{\mathcal{C}}$ *generovaný maticou* X *je KNH,*

2. *hodnosť každého riadkového vektora matice G je d a hodnosť každého riadkového vektora matice X je $n-k$,*

3. *počet kódových slov $\mathcal{C}$ hodnosti d je aspoň $k(q^m-1)$,*

4. *pre ľubovoľné $j \in \{1,\dots,n-k\}$ je $\mathrm{LO}(1, x_{1j}, \dots, x_{kj})$ $\mathbb{F}_q$-podpriestor $\mathbb{F}_{q^m}$ dimenzie $k+1$.*

Dôkaz.

1. *Pre spor predpokladajme, že $\tilde{\mathcal{C}}$ nie je KNH. Teda existuje nenulové kódové slovo $\tilde{\mathbf{c}} = \mathbf{m} \cdot X$ s hodnosťou $\mathrm{rk}(\tilde{\mathbf{c}}) < (n-k)-k+1 = n-2k+1$ pre nejaké nenulové $\mathbf{m} = (m_1,\dots,m_k) \in \mathbb{F}_{q^m}^k$. Označme $\mathbf{c} = \mathbf{m} \cdot G = (m_1,\dots,m_k,\tilde{\mathbf{c}})$ kódové slovo $\mathcal{C}$. Potom máme*

$$\begin{aligned}\mathrm{rk}(\mathbf{c}) &= \mathrm{rk}((\mathbf{m}, 0_{n-k}) + (0_k, \tilde{\mathbf{c}})) \le \mathrm{rk}((\mathbf{m}, 0_{n-k})) + \mathrm{rk}((0_k, \tilde{\mathbf{c}})) \\ &= \mathrm{rk}(\mathbf{m}) + \mathrm{rk}(\tilde{\mathbf{c}}) < k + n - 2k + 1 = n - k + 1.\end{aligned}$$

   Teda sme dostali spor s tým, že $\mathcal{C}$ je KNH. Takže aj $\tilde{\mathcal{C}}$ je KNH.

2. *Zvoľme $i \in \{1,\dots,k\}$. Potom $\delta_i \cdot G$, kde δ_i je i-ty vektor kanonickej bázy $\mathbb{F}_{q^m}^k$ nad $\mathbb{F}_{q^m}$, je i-ty riadkový vektor matice G, ktorý označíme G_i, a zároveň je to kódové slovo $\mathcal{C}$. Pretože $\mathcal{C}$ je KNH, tak nutne platí $\mathrm{rk}(G_i) \ge d$. Zároveň vieme, že prvých k zložiek vektoru G_i pozostáva z $k-1$ núl a jednej jednotky, zatiaľ čo zvyšných $n-k$ zložiek pochádza z i-teho riadkového vektora matice X. Z tohto dôvodu je hodnosť každého riadku matice X rovná aspoň $d-1 = n-k+1-1 = n-k$. Zároveň každý riadok matice X má $n-k$ prvkov, takže je hodnosti práve $n-k$. Odtiaľto už dostávame rovnosť $\mathrm{rk}(G_i) = d$.*

3. *Nech α je báza vektorového priestoru $\mathbb{F}_{q^m}$ nad $\mathbb{F}_q$. Z (b) už vieme, že každý riadkový vektor $G_i = (G_{i1},\dots,G_{in})$ matice G je hodnosti d. Zvolme ľubovoľné $c \in \mathbb{F}_{q^m} \setminus \{0\}$ a $i \in \{1,\dots,k\}$. Potom $c \cdot G_i = (c \cdot G_{i1},\dots,c \cdot G_{in})$ je kódové slovo $\mathcal{C}$ a $[c \cdot G_i]_\alpha = ([c \cdot G_{i1}]_\alpha,\dots,[c \cdot G_{in}]_\alpha) = D \cdot [G_i]_\alpha$, kde $D \in \mathbb{F}_q^{m\times m}$ je matica lineárneho operátora $\mathbf{a} \in \mathbb{F}_{q^m}^n \mapsto [c \cdot \mathbf{a}]_\alpha \in \mathbb{F}_q^{m\times n}$. Navyše, pretože $c \neq 0$, tak $[c\cdot\mathbf{a}]_\alpha = 0_{m\times n} \iff \mathbf{a} = \mathbf{o}$, a teda ide o lineárny operátor s nulovým jadrom. Z tohto dôvodu je D regulárna. Avšak násobenie regulárnou maticou nemení hodnosť, a preto má $c \cdot G_i$ tiež hodnosť d. Z tohto plynie, že počet kódových slov $\mathcal{C}$ hodnosti d je aspoň $k(q^m-1)$, kde k je počet možných volieb i a q^m-1 počet prípustných prvkov c.*

4. *Pre spor predpokladajme, že existuje $j \in \{1,\dots,n-k\}$ také, že je postupnosť $(1, x_{1j},\dots,x_{kj})$ lineárne závislá. Z lineárnej algebry vieme, že potom existujú prvky $m_0,\dots,m_k \in \mathbb{F}_q$, kde aspoň jedna hodnota z $m_0,\dots,m_k$ je nenulová, spĺňajúce $(m_0 + \sum_{i=1}^k m_i \cdot x_{ij}) = 0$. Označme $\mathbf{m} = (m_i)_{i=1}^k$ a položme $(c_1,\dots,c_n) = \mathbf{m} \cdot G \in \mathcal{C} \subset \mathbb{F}_{q^m}^n$. Teda pre $1 \le i \le k$ máme $c_i = m_i \in \mathbb{F}_q$ a z násobenia matíc dostávame $c_{k+j} = \sum_{i=1}^k m_i \cdot x_{ij} = -m_0 \in \mathbb{F}_q$. Takže*

$$\mathrm{rk}((c_1,\dots,c_k,c_{k+j})) = \mathrm{rank}\left(\begin{pmatrix} m_1 & m_2 & \dots & m_k & -m_0 \\ & & 0_{(m-1)\times(k+1)} & & \end{pmatrix}\right) = 1,$$

a preto $\mathrm{rk}((c_1,\ldots,c_n)) \leq n-k$*, keďže* $(c_{k+1},\ldots,c_{k+j-1},c_{k+j+1},\ldots,c_n)$ *má hodnosť nanajvýš* $n-k-1$*. Týmto sme dostali spor s tým, že* $\mathcal{C}$ *je KNH. Z tohto dôvodu je postupnosť* $(1,x_{1j},\ldots,x_{kj})$ *lineárne nezávislá pre všetky* $j \in \{1,\ldots,n-k\}$*, a teda generuje* $\mathbb{F}_q$*-podpriestor* $\mathbb{F}_{q^m}$ *dimenzie* $k+1$*.*

Týmto je dôkaz hotový.

□

Na záver tejto časti o kódoch najvzdialenejšej hodnosti sformulujme ešte kryptografický problém z nich vychádzajúci.

Definícia 13. *Nech* $n,k,r \in \mathbb{N}$ *a buďte* $H \in \mathbb{F}_{q^m}^{(n-k)\times n}, \mathbf{s} \in \mathbb{F}_{q^m}^{(n-k)}$*. Potom nájdenie vektoru* $\mathbf{e} \in \mathbb{F}_{q^m}^n$ *splňujúceho* $\mathrm{rk}(\mathbf{e}) = r$ *a* $\mathbf{s} = \mathbf{e}\cdot H^\top$ *nazveme* problémom dekódovania hodnostného syndrómu (DHS).

1.3 Gabidulinov kód

Pred tým, než budeme schopní popísať kryptosystém založený na KNH, tak si musíme zaviesť ešte špeciálnu skupinu kódov hodnostnej metriky, pre ktorú je známy efektívny dekódovací algoritmus. V tejto podkapitole nadviažeme na úvod druhej kapitoly článku Horlemannová-Trautmannová a kol. (2017) a druhú kapitolu článku Overbeck a kol. (2005).

Definícia 14. *Nech* $i \in \mathbb{N}$*. Potom* i-tu mocninu q nad $\mathbb{F}_{q^m}$ *značíme* $[i]$*, teda* $[i] = q^{i \bmod m}$.

V duchu značenia z predošlej definície zavedieme význačný automorfizmus telesa $\mathbb{F}_{q^m}$. Jeho dôkaz vynecháme, pretože hoci využíva iba lineárnej algebry, je mimo našich cieľov.

Tvrdenie 15 (Barto a Tůma, Veta 3.9)**.** *Zobrazenie* $\sigma_1 : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ *definované predpisom* $\sigma_1(a) = a^{[1]}$ *je* $\mathbb{F}_q$*-automorfizmom telesa* $\mathbb{F}_{q^m}$*, ktoré nazývame* Frobeniovým automorfizmom.

Dôsledok. Nech $i \in \mathbb{N}$. Potom zobrazenie $\sigma_i : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ definované predpisom $\sigma_i(a) = a^{[i]}$ je $\mathbb{F}_q$-automorfizmom telesa $\mathbb{F}_{q^m}$.

Lemma 16 (Horlemannová-Trautmannová a kol., 2017, Lemma 2.4.1)**.** *Nech* $k,m,n,N \in \mathbb{N}$ *také, že* $k \leq n \leq N \leq m$*, a* $\mathbf{g} = (g_1,\ldots,g_N) \in \mathbb{F}_{q^m}^N$*,* $\mathrm{rk}(\mathbf{g}) = n$*. Potom matica* $\left(g_j^{[i-1]}\right)_{i=1,j=1}^{k,N}$ *typu* $k \times N$ *nad telesom* $\mathbb{F}_{q^m}$ *má hodnosť* k*.*

Dôkaz predošlej lemmy je nad rámec tejto práce. Konštrukciu z nej využijeme na definovanie triedy kódov hodnostnej metriky. Dimenziu týchto kódov vieme jednoducho zvyšovať iterovaním Frobeniovho automorfizmu na generujúci vektor až po hodnosť tohto vektoru nad telesom $\mathbb{F}_q$.

Definícia 17. *Nech* $k,m,n \in \mathbb{N}, k \leq n \leq m$ *a* $\mathbf{g} = (g_1,\ldots,g_n) \in \mathbb{F}_{q^m}^n$*,* $\mathrm{rk}(\mathbf{g}) = n$*. Potom* Gabidulinov kód $\mathcal{G}$ *generovaný vektorom* $\mathbf{g}$ *definujeme ako* $[n,k]_{q^m}$*-kód hodnostnej metriky s generujúcou maticou*

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix} \in \mathbb{F}_{q^m}^{k\times n}. \tag{1.1}$$

Ďalším potrebným krokom je zavedenie skráteného značenia pre zachovanie prehľadnosti a zrozumiteľnosti.

- Gabidulinov $[n,k]_{q^m}$-kód $\mathcal{G}$ generovaný maticou G značíme $\mathcal{G} = \langle G \rangle$.
- Postupnosťou prvkov $(x_1, \ldots, x_n)$ nad $\mathbb{F}_{q^m}$ rovno rozumieme zložky vektora $\mathbf{x} \in \mathbb{F}_{q^m}^n$.
- Pre ľubovoľnú podmnožinu $J = \{j_1, \ldots, j_l\} \subseteq \{1, \ldots, n\}$ označíme vektor $(x_{j_1}, \ldots, x_{j_l}) \in \mathbb{F}_{q^m}^l$ ako $\mathbf{x}_J$. Analogicky, podmaticu pozostávajúcu zo stĺpcov, ktorých poradie prislúcha indexom J, matice $M \in \mathbb{F}_{q^m}^{k \times n}$ značíme $M_{.J}$.

Lemma 18. *Nech $n, k, l \in \mathbb{N}$. Buď $G \in \mathbb{F}_{q^m}^{k \times n}$ matica v tvare (1.1) a $T \in \mathbb{F}_q^{n \times l}$. Potom $G \cdot T = \begin{pmatrix} f_1 & \ldots & f_l \\ \vdots & \ddots & \vdots \\ f_1^{[k-1]} & \ldots & f_l^{[k-1]} \end{pmatrix}$ pre nejaké $f_1, \ldots, f_l \in \mathbb{F}_{q^m}$.*

Dôkaz. Označme matice $G = \begin{pmatrix} g_1 & \ldots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \ldots & g_n^{[k-1]} \end{pmatrix}$, $T = \begin{pmatrix} t_{11} & \ldots & t_{1l} \\ \vdots & \ddots & \vdots \\ t_{n1} & \ldots & t_{nl} \end{pmatrix}$ a položme $f_i = \sum_{j=1}^{n} g_j \cdot t_{ji}$ pre $1 \leq i \leq l$. Zvoľme $i, h \in \mathbb{N}, i \leq l$. Potom máme

$$f_i^{[h]} = \left(\sum_{j=1}^{n} g_j \cdot t_{ji} \right)^{[h]} \overset{\text{Dôsledok T. 15}}{=} \sum_{j=1}^{n} g_j^{[h]} \cdot t_{ji}^{[h]} \overset{\mathbb{F}_q\text{-aut.}}{=} \sum_{j=1}^{n} g_j^{[h]} \cdot t_{ji}, \text{ a teda}$$

$$G \cdot T = \begin{pmatrix} g_1 & \ldots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \ldots & g_n^{[k-1]} \end{pmatrix} \cdot \begin{pmatrix} t_{11} & \ldots & t_{1l} \\ \vdots & \ddots & \vdots \\ t_{n1} & \ldots & t_{nl} \end{pmatrix} = \begin{pmatrix} f_1 & \ldots & f_l \\ \vdots & \ddots & \vdots \\ f_1^{[k-1]} & \ldots & f_l^{[k-1]} \end{pmatrix}.$$

Takže sme ukázali, že aj matica $G \cdot T$ je v požadovanom špeciálnom tvare.

□

Veta 19. *Nech $k, m, n \in \mathbb{N}, k \leq n \leq m$. Pre Gabidulinovov $[n,k]_{q^m}$-kód $\mathcal{G}$ platí $d(\mathcal{G}) = n - k + 1$, teda je KNH.*

Dôkaz. Nech $G = \left(g_j^{[i-1]} \right)_{i=1,j=1}^{k,n}$ je generujúca matica kódu $\mathcal{G}$ pre nejaký vektor $\mathbf{g} \in \mathbb{F}_{q^m}^n, \mathrm{rk}(\mathbf{g}) = n$. Zvoľme maticu $V = (v_{ij}) \in \mathbb{F}_q^{k \times n}$, $\mathrm{rank}(V) = k$. Podľa lemmy 18 dostávame $G \cdot V^\top = \left(f_j^{[i-1]} \right)_{i,j=1}^{k}$, kde $f_i = \sum_{j=1}^{n} g_j \cdot v_{ij}$ $\forall i \in \mathbb{N}, i \leq k$. Pre spor predpokladajme, že $f_1, \ldots, f_k$ je lineárne závislá postupnosť nad $\mathbb{F}_q$, teda existujú $a_1, \ldots, a_k \in \mathbb{F}_q$ aspoň jedno nenulové také, že $\sum_{i=1}^{k} a_i f_i = 0$. Potom však platí $0 = \sum_{i=1}^{k} a_i f_i = \sum_{i=1}^{k} a_i \sum_{j=1}^{n} g_j \cdot v_{ij} = \sum_{j=1}^{n} \left(\sum_{i=1}^{k} a_i \cdot v_{ij} \right) g_j$. Dostali sme, že buď $g_1, \ldots, g_n$ je lineárne závislá postupnosť nad $\mathbb{F}_q$, čo je spor s $\mathrm{rk}(\mathbf{g}) = n$, alebo $\sum_{i=1}^{k} a_i \cdot v_{ij} = 0$ $\forall j \leq n \iff \sum_{i=1}^{k} a_i \cdot \mathbf{v}_i = \mathbf{o}$, kde $\mathbf{v}_i$ sú riadky V, čo je spor s $\mathrm{rank}(V) = k$. Takže $\mathrm{rk}(\mathbf{f}) = k$. Potom však podľa lemmy 16 je $\mathrm{rank}(G \cdot V^\top) = k$ a podľa tvrdenia 11 je $\mathcal{G}$ KNH, pretože V bola zvolená ľubovoľne.

□

Tvrdenie 20. *Nech $k, m, n \in \mathbb{N}, k \leq n \leq m$ a buď $\mathcal{G}$ Gabidulinov $[n,k]_{q^m}$-kód generovaný vektorom $\mathbf{g} \in \mathbb{F}_{q^m}^n, \mathrm{rk}(\mathbf{g}) = n$. Potom platí:*

1. *Pre každé $a \in \mathbb{F}_q, a \neq 0$, je $a \cdot \mathbf{g}$ generujúci vektor Gabidulinovho kódu $\mathcal{G}$.*
2. *Nech $T \in \mathbb{F}_q^{n \times n}, T$ regulárna matica, a G je generujúca matica $\mathcal{G}$. Potom $G \cdot T$ je generujúca matica Gabidulinovho kódu generovaného vektorom $\mathbf{g} \cdot T$.*
3. *Duálny kód Gabidulinovho $[n,k]_{q^m}$-kódu je Gabidulinov $[n, n-k]_{q^m}$-kód.*

Dôkaz.

1. *Zvoľme $a \in \mathbb{F}_q \setminus \{0\}$ a buď $\mathbf{g} = (g_1, \ldots, g_n)$. Potom generujúca matica pre generujúci vektor $a \cdot \mathbf{g}$ je $\begin{pmatrix} a \cdot g_1 & \ldots & a \cdot g_n \\ \vdots & \ddots & \vdots \\ a \cdot g_1^{[k-1]} & \ldots & a \cdot g_n^{[k-1]} \end{pmatrix} = a \cdot G$, kde G je generujúca matica s generujúcim vektorom $\mathbf{g}$, pretože podľa pôsledku tvrdenia 15 je $a^{[i]} = a$. Na záver pripomeňme, že priestor generovaný riadkami matice sa nezmení prenásobením matice skalárom.*
2. *Buď $T = (t_{ij})_{i,j=1}^k$. Z lemmy 18 plynie, že $G \cdot T$ je matica v tvare (1.1) pre vektor $(\sum_{j=1}^n g_j \cdot t_{j1}, \ldots, \sum_{j=1}^n g_j \cdot t_{jn}) = \mathbf{g} \cdot T$. Pretože násobenie regulárnou maticou nemení hodnosť matice, teda $\mathrm{rank}(G) = \mathrm{rank}(G \cdot T)$, tak priestory generované riadkovými vektormi matíc G a $G \cdot T$ majú rovnakú dimenziu. Takže $\langle G \cdot T \rangle$ je tiež Gabidulinov $[n,k]_{q^m}$-kód.*
3. *Dokázané v práci Gabidulin (1985, 4. kapitola).*

Tým je tvrdenie dokázané.

□

Veta 21. *Nech $n, k \in \mathbb{N}$. Pre každý Gabidulinov $[n,k]_{q^m}$-kód $\mathcal{G}$ existuje kontrolná matica $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$ v tvare $H = \begin{pmatrix} h_1 & \ldots & h_n \\ h_1^{[1]} & \ldots & h_n^{[1]} \\ \vdots & \ddots & \vdots \\ h_1^{[n-k-1]} & \ldots & h_n^{[n-k-1]} \end{pmatrix}$.*

Dôkaz. Podľa 3. bodu tvrdenia 20 je $\mathcal{G}^\perp$ Gabidulinovým $[n, n-k]_{q^m}$-kódom. Potom ale z definície Gabidulinovho kódu existuje generujúca matica G' v tvare (1.1). Pretože každá generujúca matica duálneho kódu $\mathcal{G}^\perp$ je kontrolnou maticou kódu $\mathcal{G}$, tak platí $G \cdot (G')^\top = 0_{k \times (n-k)}$. Teda stačí položiť $H = G'$.

□

Odteraz budeme za kontrolnú maticu Gabidulinovho kódu brať práve maticu H v tvare ako vo vete 21. Tento špecifický tvar kontrolnej matice sa nám už čoskoro hodí pri odvodzovaní dekódovacieho algoritmu.

1.4 Dekódovanie v Gabidulinových kódoch

Nasledujúca časť bude využívať a rozširovať poznatky 3. kapitoly práce Gabidulin (1992). Než sa však zameriame na samotný dekódovací algoritmus Gabidulinovho kódu, tak si musíme ešte osvojiť špeciálnu skupinu polynómov nad $\mathbb{F}_{q^m}$, ktoré budú kľúčové vo výpočtoch.

Definícia 22. *Nech $n \in \mathbb{N}$. Potom* linearizovaný polynóm *s koeficientami z konečného telesa $\mathbb{F}_{q^m}$ je polynóm tvaru $F(z) = \sum_{i=0}^{n} f_i z^{[i]}$. Množinu všetkých linearizovaných polynómov s koeficientami z $\mathbb{F}_{q^m}$ budeme značiť $\mathbb{R}_m[z]$.*

Poznámka. V krátkosti doplníme zaujímavé informácie o linearizovaných polynómoch, ktorých dôkazy sú však nad rámec tejto práce:

1. Množina $\mathbb{R}_m[z]$ spolu s $+$ definovaným ako $F(z) + G(z) = \sum_{i=0}^{n} (f_i + g_i) z^{[i]}$ a $*$ definovaným ako $F(z) * G(z) = \sum_{i=0}^{n} (\sum_{k+s=i} f_s \cdot g_k^{[s]}) z^{[i]}$ pre $F, G \in \mathbb{R}_m[z]$ tvorí nekomutatívny okruh (násobenie linearizovaných polynómov nie je komutatívne, dá sa naňho hľadieť ako na dosadzovanie $F(G(z))$).

2. Názov linearizované polynómy bol zvolený preto, lebo dosadenie do takýchto polynómov nad konečným telesom odpovedá $\mathbb{F}_q$-lineárnemu zobrazeniu (využíva sa Frobeniov automorfizmus).

Lemma 23. *Nech $F(z) = \sum_{i=0}^{n} F_i \cdot z^{[i]} \in \mathbb{R}_m[z]$ a $\mathcal{M}$ je množina všetkých koreňov F v $\mathbb{F}_{q^m}$. Potom $\mathcal{M}$ je podpriestor vektorového priestoru $\mathbb{F}_{q^m}$ nad telesom $\mathbb{F}_q$.*

Dôkaz. Zrejme $\mathcal{M} \subseteq \mathbb{F}_{q^m}$. Zvoľme $\alpha, \beta \in \mathcal{M}$ a $t \in \mathbb{F}_q$. Potom máme:

$$\begin{aligned} F(\alpha+\beta) &= \sum_{i=0}^{n} F_i \cdot (\alpha+\beta)^{[i]} \overset{\text{Dôsledok T. 15}}{=} \sum_{i=0}^{n} F_i \cdot (\alpha^{[i]} + \beta^{[i]}) \\ &= \sum_{i=0}^{n} F_i \cdot \alpha^{[i]} + \sum_{i=0}^{n} F_i \cdot \beta^{[i]} = F(\alpha) + F(\beta) = 0 \implies \alpha+\beta \in \mathcal{M}, \\ F(t\cdot\alpha) &= \sum_{i=0}^{n} F_i \cdot (t\cdot\alpha)^{[i]} = \sum_{i=0}^{n} F_i \cdot t^{[i]} \cdot \alpha^{[i]} \overset{\mathbb{F}_q\text{-aut.}}{=} \sum_{i=0}^{n} F_i \cdot t \cdot \alpha^{[i]} \\ &= t \cdot \sum_{i=0}^{n} F_i \cdot \alpha^{[i]} = t \cdot F(\alpha) = 0 \implies t\cdot\alpha \in \mathcal{M}. \end{aligned}$$

Využili sme, že podľa dôsledku tvrdenia 15 je umocnenie na $[i]$ $\mathbb{F}_q$-automorfizmus telesa $\mathbb{F}_{q^m}$. Tým sme ukázali, že $\mathcal{M} \subseteq \mathbb{F}_{q^m}$ je uzavretá na sčítanie v $\mathcal{M}$ a násobky prvkami $\mathbb{F}_q$, takže $\mathcal{M} \leq \mathbb{F}_{q^m}$.

□

Teraz sa pozrieme, aké vzťahy platia medzi kódovými slovami, vektorom chýb a syndrómom chyby. Tieto vzťahy využijeme na sformulovanie ideí, pomocou ktorých dokážeme popísať dekódovanie v Gabidulinových kódoch. Nech $\mathbf{c}$ je kódové slovo Gabidulinovho kódu $\mathcal{G} = \langle G \rangle$ s kontrolnou maticou H z vety 21, $\mathbf{e} \in \mathbb{F}_{q^m}^n$ je vektor chyby s hodnosťou l a $\mathbf{y} = \mathbf{c} + \mathbf{e}$ je prijatý vektor. Označme

$d = d(\mathcal{G}) = n - k + 1$. Podľa lemmy 8 existujú vektor $\mathbf{E} = (E_1, \ldots, E_l) \in \mathbb{F}_{q^m}^l$ hodnosti l a matica $Y = (Y_{ij}) \in \mathbb{F}_q^{l \times n}, \text{rank}(Y) = l$ splňujúce

$$\mathbf{e} = \mathbf{E} \cdot Y = (E_1, \ldots, E_l) \cdot Y. \tag{1.2}$$

Platnosť tohto vzťahu môžeme ďalej využiť pri výpočte chyby pomocou jej syndrómu:

$$\mathbf{s} = (s_0, \ldots, s_{d-2}) = \mathbf{y} \cdot H^\top = \mathbf{e} \cdot H^\top = \mathbf{E} \cdot Y \cdot H^\top = \mathbf{E} \cdot X, \tag{1.3}$$

kde $X = Y \cdot H^\top$ je podľa lemmy 18 pre $X^\top$ matica v tvare

$$X = \begin{pmatrix} x_1 & x_1^{[1]} & \ldots & x_1^{[d-2]} \\ x_2 & x_2^{[1]} & \ldots & x_2^{[d-2]} \\ \vdots & \vdots & \ddots & \vdots \\ x_l & x_l^{[1]} & \ldots & x_l^{[d-2]} \end{pmatrix} \text{ s prvkami } x_i = \sum_{j=1}^{n} Y_{ij} \cdot h_j, i = 1, \ldots, l, \tag{1.4}$$

ktoré sú lineárne nezávislé nad $\mathbb{F}_q$. Pretože umocnenie na $[i]$ je $\mathbb{F}_q$-lineárne zobrazenie, tak potom vzťah určený syndrómom chyby (1.3) môžeme prepísať do nasledujúcej sústavy lineárnych rovníc:

$$\sum_{j=1}^{l} E_j \cdot x_j^{[i]} = s_i, i = 0, \ldots, d-2. \tag{1.5}$$

Najprv predpokladajme, že máme riešenie $E_1, \ldots, E_l, x_1, \ldots, x_l$ systému (1.5) pre zložky syndrómu $(s_1, \ldots, s_{d-2}) = \mathbf{y} \cdot H^\top$ v zmysle predošlých úvah. Potom pre dané x_i a zložky $h_1, \ldots, h_n$ prvého riadku matice H existujú koeficienty $Y_{i1}, \ldots, Y_{in}$ v rovnici (1.4) pre $i = 1, \ldots, l$, pričom $Y_{i1}, \ldots, Y_{in} \in \mathbb{F}_q$, keďže tak bola pôvodne definovaná matica X. Tým už máme určený vektor chyby $\mathbf{e}$, pretože platí (1.2) pre vektor $(E_1, \ldots, E_l)$ a maticu $Y = (Y_{ij})$. Ďalej už je možné obnoviť pôvodnú správu $\mathbf{c} = \mathbf{y} - \mathbf{e}$. Vďaka takémuto vyjadreniu platných vzťahov a vlastností v Gabidulinových kódoch môžeme problém dekódovania previesť na hľadanie riešenia lineárnej sústavy (1.5) pre nejakú hodnosť l.

Teraz sa pozrieme, ako nájsť riešenie sústavy (1.5) splňujúce uvedené úvahy, na čo využijeme vlastností linearizovaných polynómov. Zavádzame teda polynóm $\Delta(z) = \prod_{i=1}^{l} \left(z^{[1]} - x_i^{[1]}\right) = \sum_{j=0}^{l} \Delta_j \cdot z^{[j]} \in R_m[z], \Delta_l = 1$. Podľa lemmy 23 tvoria korene polynómu Δ $\mathbb{F}_q$-podpriestor $\mathbb{F}_{q^m}$, ktorý označíme $\mathcal{M}$. Teda Δ má ako korene všetky možné $\mathbb{F}_q$-lineárne kombinácie neznámych $x_1, \ldots x_l$ zo sústavy (1.5), čiže $(x_1, \ldots x_l)$ tvorí bázu $\mathcal{M}$. Ukážeme, že vektor chyby $\mathbf{e}$ nezávisí na voľbe bázy priestoru $\mathcal{M}$, ktorú využijeme vo výpočtoch.

Lemma 24. *Nech* $\mathbf{u}$ *a* $\mathbf{v}$ *sú bázy vektorového priestoru* $\mathcal{M}$ *nad* $\mathbb{F}_q$. *Ďalej buďte* $\mathbf{E^u} = (E_1^{\mathbf{u}}, \ldots, E_l^{\mathbf{u}})$ *a* $\mathbf{E^v} = (E_1^{\mathbf{v}}, \ldots, E_l^{\mathbf{v}})$ *vektory riešení sústavy rovníc* (1.5) *a* $Y^{\mathbf{u}} = (Y_{ij}^{\mathbf{u}})_{i=1,j=1}^{l,n}, Y^{\mathbf{v}} = (Y_{ij}^{\mathbf{v}})_{i=1,j=1}^{l,n}$ *riešenia sústavy* (1.4) *pre zložky* $\mathbf{u}, \mathbf{v}$ *namiesto* $x_1, \ldots, x_l$ *v tomto poradí. Potom* $\mathbf{E^u} \cdot Y^{\mathbf{u}} = \mathbf{E^v} \cdot Y^{\mathbf{v}}$.

Dôkaz. *Označme* $\mathbf{h} = (h_1, \ldots, h_n)$ *prvý riadok kontrolnej matice* H. *Najprv si*

uvedomíme, že platí $\mathbf{u} = \mathbf{v} \cdot [id]_{\mathbf{v}}^{\mathbf{u}}$. *Potom máme:*

$$\begin{aligned}
(1.4)\ \mathbf{u} = \mathbf{h} \cdot (Y^{\mathbf{u}})^\top \ \&\ \mathbf{v} = \mathbf{h} \cdot (Y^{\mathbf{v}})^\top &\iff \mathbf{h} \cdot (Y^{\mathbf{u}})^\top = \mathbf{v} \cdot [id]_{\mathbf{v}}^{\mathbf{u}} \\
&\iff \mathbf{h} \cdot (Y^{\mathbf{u}})^\top = \mathbf{h} \cdot (Y^{\mathbf{v}})^\top \cdot [id]_{\mathbf{v}}^{\mathbf{u}} \\
&\iff (Y^{\mathbf{u}})^\top = (Y^{\mathbf{v}})^\top \cdot [id]_{\mathbf{v}}^{\mathbf{u}} \iff Y^{\mathbf{u}} = ([id]_{\mathbf{v}}^{\mathbf{u}})^\top \cdot Y^{\mathbf{v}}, \\
(1.5)\ \mathbf{u} \cdot (\mathbf{E}^{\mathbf{u}})^\top = s_0 = \mathbf{v} \cdot (\mathbf{E}^{\mathbf{v}})^\top &\iff \mathbf{v} \cdot [id]_{\mathbf{v}}^{\mathbf{u}} \cdot (\mathbf{E}^{\mathbf{u}})^\top = \mathbf{v} \cdot (\mathbf{E}^{\mathbf{v}})^\top \\
&\iff \mathbf{E}^{\mathbf{u}} \cdot ([id]_{\mathbf{v}}^{\mathbf{u}})^\top = \mathbf{E}^{\mathbf{v}} \iff \mathbf{E}^{\mathbf{u}} = \mathbf{E}^{\mathbf{v}} \cdot [([id]_{\mathbf{v}}^{\mathbf{u}})^\top]^{-1}.
\end{aligned}$$

Dokopy dostávame $\mathbf{E}^{\mathbf{u}} \cdot Y^{\mathbf{u}} = \mathbf{E}^{\mathbf{v}} \cdot [([id]_{\mathbf{v}}^{\mathbf{u}})^\top]^{-1} \cdot ([id]_{\mathbf{v}}^{\mathbf{u}})^\top \cdot Y^{\mathbf{v}} = \mathbf{E}^{\mathbf{v}} \cdot Y^{\mathbf{v}}$.

□

Ďalej nás zaujíma, aký majú vzťah koeficienty Δ_i linearizovaného polynómu Δ so súradnicami s_i syndrómu chyby.

Tvrdenie 25. *Pre ľubovoľné* $0 \leq i \leq d-2-l$ *platí rovnosť*

$$s_{i+l} + \Delta_{l-1}^{[i]} \cdot s_{i+l-1} + \cdots + \Delta_1^{[i]} \cdot s_{i+1} + \Delta_0^{[i]} \cdot s_i = 0. \tag{1.6}$$

Dôkaz. Zvoľme $0 \leq i \leq d-2-l$. *Postupne vynásobíme* i*-tu rovnicu v* (1.5) *koeficientom* $\Delta_0^{[i]}$, $(i+1)$*-vú rovnicu koeficientom* $\Delta_1^{[i]}$, …, $(i+l-1)$*-vú rovnicu koeficientom* $\Delta_{l-1}^{[i]}$ *a* $(i+l)$*-tu rovnicu koeficientom* $\Delta_l^{[i]} = 1$. *V ďalšom kroku tieto rovnice sčítame a dostaneme*

$$\sum_{k=0}^{l} \Delta_k^{[i]} \cdot s_{i+k} = \sum_{k=0}^{l} \Delta_k^{[i]} \cdot \sum_{j=1}^{l} E_j \cdot x_j^{[i+k]} = \sum_{j=1}^{l} E_j \cdot \sum_{k=0}^{l} \Delta_k^{[i]} \cdot x_j^{[k+i]}.$$

Podľa dôsledku tvrdenia 15 je umocnenie na $[i]$ *v* $\mathbb{F}_{q^m}$ $\mathbb{F}_q$*-automorfizmus, takže platí* $\sum\limits_{k=0}^{l} \Delta_k^{[i]} \cdot x_j^{[k+i]} = \sum\limits_{k=0}^{l} \left(\Delta_k x_j^{[k]}\right)^{[i]} = \left(\sum\limits_{k=0}^{l} \Delta_k x_j^{[k]}\right)^{[i]} = \left(\Delta(x_j)\right)^{[i]} = 0$, *kde sme využili, že polynóm* Δ *má koreň v* x_j, *pričom triviálne platí* $0^{[i]} = 0$. *Odtiaľto plynie, že* $\sum\limits_{k=0}^{l} \Delta_k^{[i]} \cdot s_{i+k} = 0$.

□

Poznámka. Rovnosť (1.6) vieme pre $0 \leq i \leq d-2-l$ ekvivalentne napísať v tvare

$$s_{i+l}^{[-i]} + \Delta_{l-1} \cdot s_{i+l-1}^{[-i]} + \cdots + \Delta_1 \cdot s_{i+1}^{[-i]} + \Delta_0 \cdot s_i^{[-i]} = 0, \tag{1.7}$$

kde $[-i] = q^{-i} = \frac{1}{q^i}$, takže $s_j^{[-i]}$ značí $[i]$-tu odmocninu z s_j, ktorá je jednoznačne určená, pretože to je vzor $\mathbb{F}_q$-automorfizmu $a \mapsto a^{[i]}$ telesa $\mathbb{F}_{q^m}$.

Rovnicu (1.7) môžeme ďalej použiť na zavedenie nasledujúcej sústavy rovníc, v ktorej máme ako neznáme koeficienty $\Delta_0, \ldots, \Delta_{l-1}$ polynómu Δ:

$$\begin{gathered}
(\Delta_0, \Delta_1, \ldots, \Delta_{l-1}) \cdot M_l = -(s_l, s_{l+1}^{[-1]}, \ldots, s_{2l-1}^{[-l+1]}), \\
\text{kde } M_i = \begin{pmatrix} s_0 & s_1^{[-1]} & \ldots & s_{i-1}^{[-i+1]} \\ s_1 & s_2^{[-1]} & \ldots & s_i^{[-i+1]} \\ \vdots & \vdots & \ddots & \vdots \\ s_{i-1} & s_i^{[-1]} & \ldots & s_{2i-2}^{[-i+1]} \end{pmatrix} \in \mathbb{F}_{q^m}^{i \times i}.
\end{gathered} \tag{1.8}$$

Zostáva určiť, kedy môžeme takúto sústavu rovníc jednoznačne riešiť. Z lineárnej algebry vieme, že pre štvorcovú maticu sústavy existuje jednoznačné riešenie práve vtedy, keď je matica sústavy regulárna, čo nastáva práve vtedy, keď má nenulový determinant.

Tvrdenie 26. *Ak má vektor chyby hodnosť $l \leq \frac{d-1}{2}$, potom je matica M_i regulárna pre $i = l$ a singulárna pre $i > l$.*

Dôkaz. Predpokladajme, že máme $E_1, \ldots, E_l$ z (1.2) a $x_1, \ldots, x_l$ z (1.4). Dodefinujme $E_i = 0$ a $x_i = 0$ pre $i > l$. Zvoľme $0 \leq a \leq d-2$ a $b \in \mathbb{N}$. Umocnením rovnice (1.5) na $[-b]$ a využitím, že umocnenie na $[-b] = [m-b]$ je $\mathbb{F}_q$-lineárne zobrazenie, dostávame:

$$s_a^{[-b]} \overset{(1.5)}{=} \left(\sum_{j=1}^{l} E_j \cdot x_j^{[a]} \right)^{[-b]} = \sum_{j=1}^{l} \left(E_j \cdot x_j^{[a]} \right)^{[-b]} = \sum_{j=1}^{l} E_j^{[-b]} \cdot x_j^{[a-b]}.$$

Potom maticu M_i v (1.8) vieme pomocou predošlého vzťahu vyjadriť v tvare

$$M_i = \underbrace{\begin{pmatrix} x_1 & x_2 & \ldots & x_i \\ x_1^{[1]} & x_2^{[1]} & \ldots & x_i^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{[i-1]} & x_2^{[i-1]} & \ldots & x_i^{[i-1]} \end{pmatrix}}_{X^i} \cdot \underbrace{\begin{pmatrix} E_1 & E_1^{[-1]} & \ldots & E_1^{[-i+1]} \\ E_2 & E_2^{[-1]} & \ldots & E_2^{[-i+1]} \\ \vdots & \vdots & \ddots & \vdots \\ E_i & E_i^{[-1]} & \ldots & E_i^{[-i+1]} \end{pmatrix}}_{E^i}.$$

Pre $i > l$ obsahuje matica X^i nulové stĺpce a matica E^i nulové riadky, čiže obe matice sú singulárne, a teda aj M_i je singulárna. Pretože $\mathrm{rk}((E_1, \ldots, E_l)) = l$ a $\mathrm{rk}((x_1, \ldots, x_l)) = l$ priamo z ich voľby, tak pre $i = l$ sú matice X^l a $(E^l)^\top$ regulárne podľa lemmy 16. Potom aj M_l je regulárna matica.

□

Dôsledok. Gabidulinov $[n,k]_{q^m}$-kód $\mathcal{G}$ opravuje $\left\lfloor \frac{n-k}{2} \right\rfloor = \left\lfloor \frac{d(\mathcal{G})-1}{2} \right\rfloor$ chýb.

Teraz už len zhrnieme poznatky získané v tejto podkapitole týkajúce sa vzťahov medzi kódovým slovom zaťaženým vektorom chyby a daným syndrómom chyby v dvoch algoritmoch, ktoré nám popisujú proces dekódovania v Gabidulinovom kóde $\mathcal{G}$ generovaného maticou G s kontrolnou maticou H.

1. **Algoritmus určenia chyby $\mathcal{CH}_\mathcal{G}$**
   Vstup: syndróm chyby $\mathbf{s} = (s_0, \ldots, s_{d-2})$
   Výstup: vektor chyby $\mathbf{e}$

   (a) Určíme najväčšie celé číslo $t \leq \frac{d-1}{2}$ také, že $\det(M_t) \neq 0$ pre maticu $M_t = (s_{i+j}^{[-j]})_{i,j=0}^{t-1}$. Podľa tvrdenia 26 takéto t existuje.

   (b) Vyriešime sústavu lineárnych rovníc (1.8) pre neznáme $\Delta_0, \ldots, \Delta_{t-1}$ a položíme $\Delta_t = 1$.

   (c) Nech $\mathcal{M}$ je množina koreňov polynómu $\Delta(z) = \sum_{i=0}^{t} \Delta_i \cdot z^{[i]} \in \mathbb{R}_m[z]$, čiže $\mathcal{M}$ je jadrom $\mathbb{F}_q$-lineárneho zobrazenia Δ. Vyriešením príslušnej homogénnej sústavy rovníc nájdeme bázu $(x_1, \ldots, x_t)$ podpriestoru $\mathcal{M}$ vektorového priestoru $\mathbb{F}_{q^m}$ nad $\mathbb{F}_q$.

(d) Vyriešime sústavu lineárnych rovníc (1.5) pre neznáme $E_1, \ldots, E_t$.

(e) Pre všetky $1 \leq i \leq t$ vyriešime sústavu rovníc (1.4) v neznámych $Y_{i1}, \ldots, Y_{in} \in \mathbb{F}_q$ pomocou matice sústavy $([h_1]_\alpha \ \ldots \ [h_n]_\alpha \mid [x_i]_\alpha)$, kde α je nejaká báza priestoru $\mathbb{F}_{q^m}$ nad $\mathbb{F}_q$, pričom $Y_{i1}, \ldots, Y_{in}$ nie sú závislé na α.

(f) Z vypočítaného vektora $\mathbf{E} = (E_1, \ldots, E_t)$ a matice $Y = (Y_{ij})_{i=1,j=1}^{t,n}$ spočítame vektor chyby $\mathbf{e} = \mathbf{E} \cdot Y$, ktorý je podľa lemmy 24 určený jednoznačne.

2. **Dekódovací algoritmus $\mathcal{D}_\mathcal{G}$**
Vstup: prijatý vektor $\mathbf{y} = \mathbf{c} + \mathbf{e}$, kde $\mathbf{c} \in \mathcal{G}$ a $\mathbf{e}$ je vektor chyby
Výstup: pôvodná správa $\mathbf{c}$

(a) Spočítame syndróm $\mathbf{s} = (s_0, \ldots, s_{d-2}) = \mathbf{y} \cdot H^\top$.

(b) Aplikujeme algoritmus určenia chyby na syndróm $\mathbf{s}$ a dostaneme vektor chyby $\mathbf{e} = \mathcal{CH}_\mathcal{G}(\mathbf{s})$.

(c) Určíme pôvodnú správu $\mathbf{c} = \mathbf{y} - \mathbf{e}$.

2. Kryptografické systémy

Pred predstavením kryptosystému založeného na kódoch hodnostnej metriky je potrebné formálne zaviesť nevyhnutné pojmy z kryptografie.

Definícia 27. Asymetrický kryptosystém *je usporiadaná pätica konečných množín* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, e, d)$*, kde:*

- $\mathcal{P}$ *je* množina otvorených textov*,*
- $\mathcal{C}$ *je* množina šifrovaných textov*,*
- $\mathcal{K} = \{(\mathbf{k}, p(\mathbf{k})) \mid \mathbf{k} \in \mathcal{K}_\mathcal{S}\}$ *je* priestor kľúčov*, kde* $\mathcal{K}_\mathcal{S}$ *je* priestor súkromných (tajných) kľúčov*,* $\mathcal{K}_\mathcal{V}$ *je* priestor verejných (známych) kľúčov *a* $p : \mathcal{K}_\mathcal{S} \to \mathcal{K}_\mathcal{V}$ *je zobrazenie, ktoré súkromnému kľúču priraďuje k nemu príslušný verejný kľúč,*
- $e : \mathcal{P} \times \mathcal{K}_\mathcal{V} \to \mathcal{C}$ *je* šifrovacie zobrazenie*,*
- $d : \mathcal{C} \times \mathcal{K}_\mathcal{S} \to \mathcal{P}$ *je* dešifrovacie zobrazenie*.*

Pre každú správu $\mathbf{m} \in \mathcal{P}$ *a každý kľúč* $(\mathbf{k}, p(\mathbf{k})) \in \mathcal{K}$ *musí platiť*

$$d(e(\mathbf{m}, p(\mathbf{k})), \mathbf{k}) = \mathbf{m}.$$

Majme dvoch účastníkov komunikácie, označme ich A a B, ktorí chcú bezpečne komunikovať. Ak chce účastník A poslať správu $\mathbf{m}$ účastníkovi B pomocou asymetrického kryptosystému, tak musí poznať verejný kľúč $\mathbf{k}_\mathcal{V}^\mathbf{B}$ účastníka B. Potom môže vytvoriť šifrovanú správu $\mathbf{c} = e(\mathbf{m}, \mathbf{k}_\mathcal{V}^\mathbf{B})$ a poslať ju B. Účastník B obdrží šifrovanú správu $\mathbf{c}$, ktorú môže dešifrovať svojím súkromným kľúčom $\mathbf{k}_\mathcal{S}^\mathbf{B}$. Takže B sa pomerne ľahko a bezpečne dostane k správe $\mathbf{m} = d(\mathbf{c}, \mathbf{k}_\mathcal{S}^\mathbf{B})$.

V nasledujúcich podkapitolách popíšeme a overíme správnosť schém asymetrických kryptosystémov z 3. kapitoly článku Overbeck a kol. (2005).

2.1 GPT kryptosystém

Pôvodný GPT kryptosystém bol predstavený v roku 1991 pánmi Gabidulinom, Paramonovom a Tretjakovom. Úplne prvá verzia tohto asymetrického kryptosystému bola založená na McElieceovom kryptosystéme s určitými modifikáciami pre efektívne použitie KNH. Najprv sa zvolila generujúca matica G Gabidulinovho $[n, k]_{q^m}$-kódu opravujúceho $t = \lfloor \frac{n-k}{2} \rfloor$ chýb, $S \in \mathbb{F}_{q^m}^{k \times k}$ regulárna matica určená na zakódovanie štruktúry G a matica $X \in \mathbb{F}_{q^m}^{k \times n}$ hodnosti $t_X < t$ na zamaskovanie štruktúry $S \cdot G$. Ako verejný kľúc sa zverejnila matica $V = S \cdot G + X$ spolu s hodnosťou t_X, súkromný kľúč pozostával z dekódovacieho algoritmu $\mathcal{G}$ a matíc S, G. Pre zašifrovanie k-bitovej správy m sa vypočítal šifrový text ako $\mathbf{c} = m \cdot V + \mathbf{e}$, kde $\mathbf{e} \in \mathbb{F}_{q^m}^n, \mathrm{rk}(\mathbf{e}) \leq t - t_X$ bol náhodne zvolený vektor chyby. Legitímny príjemnca dekódovacím algoritmom dostal zo šifrového textu $\mathbf{c}$ kódové slovo $m \cdot S \cdot G$, z ktorého už jednoducho dopočítal správu m.

V tejto podkapitole presne popíšeme zobecnenú verziu GPT kryptosystému, takzvaný generalizovaný GPT (GGPT). Hlavný rozdiel oproti pôvodnému GPT kryptosystému spočíva v snahe bezpečnejšie skryť štruktúru generujúcej matice.

- **Voľba parametrov:** Nech q je prvočíslo a $k, n, m, t, s \in \mathbb{N} : k < n \leq m$ a $s \leq \min\{t, k\}$.
- **Generovanie kľúča:** Ako prvé generujeme nasledovné matice:

$G \in \mathbb{F}_{q^m}^{k \times n}$	matica generujúca Gabidulinov $[n,k]_{q^m}$-kód $\mathcal{G}$,
$X \in \mathbb{F}_{q^m}^{k \times t}$	matica splňujúca $\operatorname{rank}(X) = s$ a $\operatorname{rank}_q^{\downarrow}(X) = t$,
$S \in \mathbb{F}_{q^m}^{k \times k}$	náhodná regulárna matica (kódovač riadkov) a
$T \in \mathbb{F}_q^{(n+t)\times(n+t)}$	náhodná regulárna matica (kódovač stĺpcov).

  Ďalej položme maticu $G^{\mathcal{V}} = S \cdot \begin{bmatrix} X & G \end{bmatrix} \cdot T \in \mathbb{F}_{q^m}^{k \times (n+t)}$ typu $k \times (n+t)$. Zvolíme $1 \leq e \leq \frac{n-k}{2}$ a označíme $\mathcal{D}_{\mathcal{G}}$ efektívny dekódovací algoritmus Gabidulinovho $[n,k]_{q^m}$-kódu $\mathcal{G}$ (2. algoritmus na konci podkapitoly 1.3).
- **Verejný kľúč:** $\mathcal{K}_{\mathcal{V}} = (G^{\mathcal{V}}, e)$
- **Súkromný kľúč:** $\mathcal{K}_{\mathcal{S}} = (\mathcal{D}_{\mathcal{G}}, G, S, T)$,
- **Šifrovanie:** Máme správu $\mathbf{x} \in \mathbb{F}_{q^m}^k$ a náhodne zvolíme vektor $\mathbf{z} \in \mathbb{F}_{q^m}^{n+t}$ hodnosti $\operatorname{rk}(\mathbf{z}) \leq e$. Šifrový text $\mathbf{c}$ spočítame ako $\mathbf{c} = \mathbf{x} \cdot G^{\mathcal{V}} + \mathbf{z}$.
- **Dešifrovanie:** Aby sme dešifrovali $\mathbf{c}$, tak použijeme dekódovací algoritmus $\mathcal{D}_{\mathcal{G}}$ Gabidulinovho kódu $\mathcal{G}$ na vektor $\mathbf{c}' = (\mathbf{c} \cdot T^{-1})_{\{t+1,\ldots,n+t\}}$. Pretože T je regulárna, a teda invertibilná nad $\mathbb{F}_q$, tak hodnosť vektora sa nezmení prenásobením maticou T^{-1}. Preto má $\mathbf{c}'$ hodnostnú vzdialenosť od $\mathcal{G}$ najviac $\frac{n-k}{2}$. Aplikovaním dekódovacieho algoritmu kódu $\mathcal{G}$ na $\mathbf{c}'$ dostávame $\mathcal{D}_{\mathcal{G}}(\mathbf{c}') = \mathbf{x} \cdot S \cdot G$, z ktorého vieme určiť pôvodnú správu $\mathbf{x}$ ako riešenie sústavy lineárnych rovníc.

Lemma 28. *Dešifrovanie GPT funguje.*

Dôkaz. Budeme využívať vyššie zavedeného značenia. Najprv si vyjadríme $\mathbf{c} \cdot T^{-1}$ *a ako tento vektor vyzerá bez prvých* t *zložiek:*

$$\begin{aligned}
\mathbf{c} \cdot T^{-1} &= (\mathbf{x} \cdot G^{\mathcal{V}} + \mathbf{z}) \cdot T^{-1} = \mathbf{x} \cdot S \cdot \begin{bmatrix} X & G \end{bmatrix} \cdot T \cdot T^{-1} + \mathbf{z} \cdot T^{-1} \\
&= \mathbf{x} \cdot S \cdot \begin{bmatrix} X & G \end{bmatrix} + \mathbf{z} \cdot T^{-1}, \\
\mathbf{c}' &= (\mathbf{c} \cdot T^{-1})_{\{t+1,\ldots,n+t\}} = (\mathbf{x} \cdot S \cdot \begin{bmatrix} X & G \end{bmatrix} + \mathbf{z} \cdot T^{-1})_{\{t+1,\ldots,n+t\}} \\
&= \left(\mathbf{x} \cdot S \cdot \begin{bmatrix} X & G \end{bmatrix}\right)_{\{t+1,\ldots,n+t\}} + (\mathbf{z} \cdot T^{-1})_{\{t+1,\ldots,n+t\}} \\
&= (\mathbf{x} \cdot S) \cdot \begin{bmatrix} X & G \end{bmatrix}_{.\{t+1,\ldots,n+t\}} + (\mathbf{z} \cdot T^{-1})_{\{t+1,\ldots,n+t\}} \\
&= (\mathbf{x} \cdot S) \cdot G + (\mathbf{z} \cdot T^{-1})_{\{t+1,\ldots,n+t\}}.
\end{aligned}$$

Využili sme, že $\left(\mathbf{x} \cdot S \cdot \begin{bmatrix} X & G \end{bmatrix}\right)_{\{t+1,\ldots,n+t\}} = (\mathbf{x} \cdot S) \cdot \begin{bmatrix} X & G \end{bmatrix}_{.\{t+1,\ldots,n+t\}}$*, čo je jasné z násobenia vektora* $x \cdot S$ *s maticou* $\begin{bmatrix} X & G \end{bmatrix}$*, a* $\begin{bmatrix} X & G \end{bmatrix}_{.\{t+1,\ldots,n+t\}} = G$*. Ďalej platí* $\operatorname{rk}((\mathbf{z} \cdot T^{-1})_{\{t+1,\ldots,n+t\}}) \leq \operatorname{rk}(\mathbf{z} \cdot T^{-1}) = \operatorname{rk}(\mathbf{z}) \leq e \leq \frac{n-k}{2}$*, pretože odstránením zložiek vektora sa maximálny počet lineárne nezávislých zložiek tohto vektora môže len zmenšiť a pretože násobenie regulárnou maticou nemení hodnosť. Tým sme*

ale ukázali, že dekódovací algoritmus $\mathcal{D}_\mathcal{G}$ je podľa dôsledku tvrdenia 26 schopný odstrániť vektor chyby, a teda $\mathcal{D}_\mathcal{G}(\mathbf{c}') = \mathbf{x} \cdot S \cdot G$. Odtiaľto už vieme jednoznačne určiť pôvodnú správu $\mathbf{x}$ ako riešenie sústavy lineárnych rovníc $\mathbf{x} \cdot S \cdot G = \mathcal{D}_\mathcal{G}(\mathbf{c}')$. □

Všimnime si, že maticu S pri dešifrovaní správy $\mathbf{c}$ nemusíme poznať, pretože $S \cdot G = (G^\mathcal{V} \cdot T^{-1})_{.\{t+1,\ldots,n+t\}}$, a teda správu $\mathbf{x}$ určíme vyriešením lineárnej sústavy $\mathbf{x} \cdot (G^\mathcal{V} \cdot T^{-1})_{.\{t+1,\ldots,n+t\}} = \mathcal{D}_\mathcal{G}(\mathbf{c}')$. Z toho plynie, že pre šetrenie pamäťou nemusí byť S obsiahnuté v $\mathcal{K}_\mathcal{S}$.

2.2 Modifikácia Niederreiterovej schémy

Hlavným rozdielom oproti McElieceovej schéme kryptosystému s verejným kľúčom je, že správu nemaskujeme náhodným vektorom chyby, ale v Niederreiterovom kryptosystéme priamo vektor chyby zodpovedá správe otvoreného textu. Analogicky, pri dešifrovaní nie je cieľom odstrániť vektor chyby, ale iba ho určiť.

- **Voľba parametrov:** q prvočíslo, $k, l, n, m \in \mathbb{N} : l < k < n \leq m$, l párne.
- **Generovanie kľúča:** Ako prvé generujeme nasledovné matice:

$H \in \mathbb{F}_{q^m}^{(n-k)\times n}$	kontrolná matica Gab. $[n,k]_{q^m}$-kódu $\mathcal{G}$,
$A \in \mathbb{F}_{q^m}^{l\times n}$	matica hodnosti l nad $\mathbb{F}_{q^m}$,
$S \in \mathbb{F}_{q^m}^{(n-k+l)\times(n-k+l)}$	náhodná regulárna matica.

  Ďalej spočítame maticu typu $(n-k+l) \times n$

  $$H_\mathcal{V} = S \cdot \begin{bmatrix} H \\ A \end{bmatrix} \in \mathbb{F}_{q^m}^{(n-k+l)\times n}.$$

  Zvolíme $1 \leq e \leq \frac{n-k}{2}$ a označíme $\mathcal{CH}_\mathcal{G}$ algoritmus určenia chyby Gabidulinovho $[n,k]_{q^m}$-kódu $\mathcal{G}$ (1. algoritmus na konci podkapitoly 1.3).
- **Verejný kľúč:** $\mathcal{K}_\mathcal{V} = (H_\mathcal{V}, e)$
- **Súkromný kľúč:** $\mathcal{K}_\mathcal{S} = (\mathcal{CH}_\mathcal{G}, S)$
- **Šifrovanie:** Máme správu $\mathbf{x} \in \mathbb{F}_{q^m}^n$ hodnosti $\mathrm{rk}(\mathbf{x}) \leq e$. Šifrový text $\mathbf{c}$ spočítame ako $\mathbf{c} = \mathbf{x} \cdot H_\mathcal{V}^\top$.
- **Dešifrovanie:** Aby sme dešifrovali $\mathbf{c}$, tak najprv musíme určiť syndróm chyby $\mathbf{c}' = [\mathbf{c} \cdot (S^\top)^{-1}]_{\{1,\ldots,n-k\}}$. Následne použijeme algoritmus určenia chyby $\mathcal{CH}_\mathcal{G}$ Gabidulinovho kódu $\mathcal{G}$ na syndróm $\mathbf{c}'$, čím dostaneme pôvodnú správu $\mathbf{x} = \mathcal{CH}_\mathcal{G}(\mathbf{c}')$.

Lemma 29. *Dešifrovanie Niederreiterovej schémy pre GPT funguje.*

Dôkaz. Najprv overíme, že platí $\mathbf{c}' = \mathbf{x} \cdot H^\top$:

$$\begin{aligned}
\mathbf{c} \cdot (S^\top)^{-1} &= \mathbf{x} \cdot H_\mathcal{V}^\top \cdot (S^\top)^{-1} = \mathbf{x} \cdot (S \cdot [\,{}^{H}_{A}\,])^\top \cdot (S^\top)^{-1} \\
&= \mathbf{x} \cdot \begin{bmatrix} H^T & A^T \end{bmatrix} \cdot S^\top \cdot (S^\top)^{-1} = \mathbf{x} \cdot \begin{bmatrix} H^T & A^T \end{bmatrix} = \left(\mathbf{x} \cdot H^T,\, \mathbf{x} \cdot A^T\right), \\
\mathbf{c}' &= [\mathbf{c} \cdot (S^\top)^{-1}]_{\{1,\ldots,n-k\}} = \left(\mathbf{x} \cdot H^T,\, \mathbf{x} \cdot A^T\right)_{\{1,\ldots,n-k\}} = \mathbf{x} \cdot H^\top.
\end{aligned}$$

Takže vstupom algoritmu $\mathcal{CH}_\mathcal{G}$ pri dešifrovaní je naozaj syndróm chyby. Pretože $\mathrm{rank}(\mathbf{x}) \leq e \leq \frac{n-k}{2}$*, tak potom podľa tvrdenia* 26 *nájde algoritmus v prvom kroku* $t = \mathrm{rk}(\mathbf{x})$*. Na záver len pripomeňme, že vektor chyby* $\mathbf{e}' = \mathcal{CH}_\mathcal{G}(\mathbf{c}')$ *je podľa lemmy 24 určený jednoznačne. Preto platí* $\mathbf{x} = \mathbf{e}'$*.*

□

Zostáva nám určiť, ako voliť maticu A, aby bolo zlomenie tohto variantu GPT čo najnáročnejšie. Využijeme poznatky zo štvrtej kapitoly práce Berger a Loidreau (2002). Najprv poznamenajme, že matica $H_\mathcal{V}$ nemôže byť kontrolnou maticou Gabidulinovho kódu, pretože potom by pre ňu existoval efektívny dekódovací algoritmus. V dôsledku tohto chceme zvoliť A tak, aby $H_\mathcal{V}$ nebola kontrolnou maticou KNH kódu, pretože potom už podľa vety 19 nemôže byť ani kontrolnou maticou Gabidulinovho kódu. Označme $\mathbf{a_1}, \ldots, \mathbf{a_l}$ riadkové vektory matice A. Potom môžeme maticu A skonštruovať nasledovne:

1. Zvolíme náhodne maticu $S_0 \in \mathbb{F}_q^{(n-k+\frac{l}{2})\times n}$ hodnosti $n-k+\frac{l}{2}$.
2. Zvolíme náhodne lineárne nezávislé vektory $\mathbf{a_1}, \ldots, \mathbf{a_{\frac{l}{2}}} \in \mathbb{F}_{q^m}^n$ také, že každý má najväčšiu možnú hodnosť nad $\mathbb{F}_q$.
3. Zvolíme zvyšné vektory $\mathbf{a_{\frac{l}{2}+1}}, \ldots, \mathbf{a_l} \in \mathbb{F}_{q^m}^n$ tak, aby pre každé $i = 1, \ldots, \frac{l}{2}$ platilo $S_0 \cdot (a_i - a_{i+\frac{l}{2}})^\top = 0$. Z lineárnej algebry vieme ľahko určiť počet riešení týchto homogénnych rovníc nad $\mathbb{F}_q$, teda $|\ker(S_0)|$. Pretože z voľby S_0 je $\mathrm{rank}(S_0) = n-k+\frac{l}{2}$, tak počet riešení tejto homogénnej rovnice pre dané $i \in \{1, \ldots, \frac{l}{2}\}$ je $|\ker(S_0)| = q^{n-\mathrm{rank}(S_0)} = q^{k-\frac{l}{2}}$. Odtiaľto plynie, že máme $q^{\frac{l}{2}(k-\frac{l}{2})}$ možností na voľbu zvyšných riadkov matice A.

Pre takto zvolené A je hodnosť $\mathrm{rank}(S_0 \cdot A^\top) \leq \frac{l}{2}$ pretože matica $S_0 \cdot A^\top$ má aspoň $\frac{l}{2}$ lineárne závislých stĺpcových vektorov. Ďalej podľa vlastností hodnosti a definície kontrolnej matice $\mathrm{rank}(S_0 \cdot H^\top) \leq \mathrm{rank}(H^\top) = n-k$. Dohromady dostávame $\mathrm{rank}\left(S_0 \cdot \begin{bmatrix} H^T & A^T \end{bmatrix}\right) \leq \mathrm{rank}(S_0 \cdot H^\top) + \mathrm{rank}(S_0 \cdot A^\top) \leq n-k+\frac{l}{2}$. Pretože násobenie regulárnou maticou nemení hodnosť, tak i $\mathrm{rank}(S_0 \cdot H_\mathcal{V}^\top) = \mathrm{rank}\left(S_0 \cdot \begin{bmatrix} H^T & A^T \end{bmatrix} \cdot S^\top\right) \leq n-k+\frac{l}{2}$. Potom ale pre $[n, k-l]_{q^m}$-kód $\mathcal{C}$ s kontrolnou maticou $H_\mathcal{V}$ je $d(\mathcal{C}) \leq n-k+\frac{l}{2} < n-k+l+1 = n-\dim(\mathcal{C})+1$. Takže $\mathcal{C}$ nie je KNH.

3. Útoky na GPT kryptosystém

Hlavnou slabinou GPT kryptosystému je náročnosť skrytia štruktúry generujúcej matice Gabidulinovho kódu. Majme nejakú maticu M, potom ako $M^{(j)}$ budeme značiť maticu, ktorá vznikla umocnením všetkých prvkov matice M na j. Nech G je generujúca matica Gabidulinovho kódu generovaného vektorom $\mathbf{g}$. Potom matice $G, G^{(j)}$ majú veľmi podobnú štruktúru, keďže $G^{(j)}$ je zrejme generujúca matica Gabidulinovho kódu generovaného vektorom $\mathbf{g}^{(j)}$. Túto vlastnosť neskôr využijeme na rozpoznanie matice generujúcej Gabidulinov kód od náhodnej v $G^{\mathcal{V}}$.

Definícia 30. *Nech $l, n, f \in \mathbb{N}$. Potom zobrazenie $\Lambda_f : \mathbb{F}_{q^m}^{l\times n} \to \mathbb{F}_{q^m}^{[(f+1)l]\times n}$ definujeme predpisom $\Lambda_f(M) = \begin{bmatrix} M \\ M^{([1])} \\ \vdots \\ M^{([f])} \end{bmatrix}$ pre $M \in \mathbb{F}_{q^m}^{l\times n}$.*

Teda zobrazenie Λ_f zobrazí maticu $M \in \mathbb{F}_{q^m}^{l\times n}$ na blokovú maticu $[(f+1)l]\times n$, kde $(i+1)$-vý blok vznikne aplikovaním i iterácii Frobeniovho $\mathbb{F}_q$-automorfizmu telesa $\mathbb{F}_{q^m}$ na prvky matice M pre $0 \leq i \leq f$.

Lemma 31. *Nech $k, m, n, f \in \mathbb{N}, k \leq n \leq m, f \leq n-k-1$ a riadky matice $M \in \mathbb{F}_{q^m}^{k\times n}$ generujú Gabidulinov $[n,k]_{q^m}$-kód $\mathcal{G}$ generovaný vektorom $\mathbf{g} \in \mathbb{F}_{q^m}^n$. Potom riadky matice $\Lambda_f(M)$ generujú Gabidulinov $[n, k+f]_{q^m}$-kód generovaný vektorom $\mathbf{g}$.*

Dôkaz. Nech $G \in \mathbb{F}_{q^m}^{k\times n}$ je generujúca matica $\mathcal{G}$ v tvare (1.1). Potom existuje regulárna matica $S \in \mathbb{F}_{q^m}^{k\times k}$ taká, že $M = S \cdot G$, pretože riadky matíc M a G generujú rovnaký priestor. Takže aj riadky matíc $\Lambda_f(M)$ a $\Lambda_f(G)$ generujú rovnaký vektorový priestor. Ďalej pre $i < f$ podľa lemmy 16 platí, že vždy iba posledný riadok $\Lambda_i(G)$, ktorý je v tvare $g^{([k-1+i])}$, neleží v lineárnom obale riadkov matice $\Lambda_{i-1}(G)$, čiže $\mathbf{g}^{([k-1+i])} \notin \mathrm{LO}(\mathbf{g}, \mathbf{g}^{([1])}, \ldots, \mathbf{g}^{([k-2+i])})$. Takže $\mathrm{rank}(\Lambda_f(G)) = f+k$, pretože $f+k < n \leq m$. Čiže riadky matice $\Lambda_f(M)$ generujú Gabidulinov $[n, k+f]_{q^m}$-kód. □

3.1 Overbeckov útok

Cieľom útoku, ktorý bol predstavený v kapitole 4.2 článku Overbeck a kol. (2005), je z verejného kľúča GPT kryptosystému $\mathcal{K}_{\mathcal{V}} = (G^{\mathcal{V}}, e)$ skonštruovať nejaký nový platný (v zmysle dešifrovania správ šifrovaných $\mathcal{K}_{\mathcal{V}}$) súkromný kľúč $\mathcal{K}_{\mathcal{S}}^{\mathcal{F}}$ operujúci s Gabidulinovým kódom s rovnakými parametrami ako mal kód $\mathcal{G}$ generovaný maticou G v pôvodnom súkromnom kľúči $\mathcal{K}_{\mathcal{S}} = (\mathcal{D}_{\mathcal{G}}, G, S, T)$.

Najprv skonštruujeme rozšírenú generujúcu maticu z generujúcej matice verejného kľúča $G^{\mathcal{V}} = S \cdot \begin{bmatrix} X & G \end{bmatrix} \cdot T$ pre $u = n-k-1$:

$$G_R^{\mathcal{V}} = \Lambda_u(G^{\mathcal{V}}) = \begin{bmatrix} G^{\mathcal{V}} \\ (G^{\mathcal{V}})^{([1])} \\ \vdots \\ (G^{\mathcal{V}})^{([u])} \end{bmatrix} = \begin{bmatrix} S & \cdot & [& X & G &] & \cdot & T \\ S^{([1])} & \cdot & [& X^{([1])} & G^{([1])} &] & \cdot & T \\ \vdots & & & \vdots & \vdots & & & \vdots \\ S^{([u])} & \cdot & [& X^{([u])} & G^{([u])} &] & \cdot & T \end{bmatrix} \tag{3.1}$$
$$= S_R \cdot \begin{bmatrix} X_R & G_R \end{bmatrix} \cdot T,$$

kde sme využili, že $T^{([j])} = T$ pre ľubovoľné j, keďže $T \in \mathbb{F}_q^{(n+t)\times(n+t)}$, a označili ako $S_R = \mathrm{diag}(S, S^{([1])}, \ldots, S^{([u])}), X_R = \Lambda_u(X)$ a $G_R = \Lambda_u(G)$. Podľa lemmy 31 pre $f = u = n-k-1$ generujú riadky matice $G_R = \Lambda_u(G)$ Gabidulinov $[n, k+f]_{q^m} = [n, n-1]_{q^m}$-kód generovaný rovnakým vektorom ako $\mathcal{G} = \langle G \rangle$, označme ho $\mathbf{g} = (g_1, \ldots, g_n)$. Položme $G_{n-1} = \left(g_j^{[i-1]}\right)_{i=1,j=1}^{n-1,n} \in \mathbb{F}_{q^m}^{(n-1)\times n}$ maticu generujúcu tento Gabidulinov $[n, n-1]_{q^m}$-kód. Potom existuje konečná postupnosť elementárnych riadkových úprav, ktorými prevedieme maticu $G_R^{\mathcal{V}}$ v (3.1) do tvaru

$$\tilde{G}_R^{\mathcal{V}} = \tilde{S}_R \cdot \begin{bmatrix} Z & G_{n-1} \\ Y_R & 0_{u(k-1)\times n} \end{bmatrix} \cdot T, \tag{3.2}$$

kde $Z \in \mathbb{F}_{q^m}^{(n-1)\times t}$ a $Y_R \in \mathbb{F}_{q^m}^{u(k-1)\times t}$. Zároveň triviálne platí, že riadky matice $G_R^{\mathcal{V}}$ a matice $\tilde{G}_R^{\mathcal{V}}$ generujú rovnaký priestor.

Lemma 32. *Nech $X_1, X_2 \in \mathbb{F}_{q^m}^{(k-1)\times t}$ sú matice, ktoré dostaneme z X vynechaním posledného riadku pre X_1 a prvého riadku pre X_2. Označme $Y = X_1^{([1])} - X_2$ maticu typu $(k-1)\times t$ nad $\mathbb{F}_{q^m}$. Potom existuje matica $Z \in \mathbb{F}_{q^m}^{(n-1)\times t}$ taká, že pre maticu $\Lambda_{u-1}(Y) = Y_R$ platí* (3.2).

Dôkaz. Nech G_u je matica typu $u(k-1)\times n$, ktorú dostaneme z podmatice G_R rovnakými riadkovými úpravami, ktorými sme dostali $\Lambda_{u-1}(Y)$ z podmatice X_R. Podľa lemmy 31 vieme, že riadky matice G_R generujú $[n, n-1]_{q^m}$-kód, a teda $\mathrm{rank}(G_R) = n-1$. *Overíme, že G_u je nulová matica. Potom nutne G_{n-1} je matica hodnosti $n-1$ a teda platí* (3.2). *Zvoľme $0 \le j \le u-1$ a pozrieme sa, ako vyzerá j-ty blok G_u, ktorý označme G_{u_j}. Teda máme:*

$$\Lambda_{u-1}(Y) = \begin{bmatrix} Y \\ Y^{([1])} \\ \vdots \\ Y^{([u-1])} \end{bmatrix} = \begin{bmatrix} X_1^{([1])} - X_2 \\ X_1^{([2])} - X_2^{([1])} \\ \vdots \\ X_1^{([u])} - X_2^{([u-1])} \end{bmatrix},$$

$$G_{u_j} = \left[\begin{pmatrix} g_1 & \cdots & g_n \\ \vdots & \ddots & \vdots \\ g_1^{[k-2]} & \cdots & g_n^{[k-2]} \end{pmatrix}^{([j])} - \begin{pmatrix} g_1^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}^{([j-1])} \right]$$
$$= \left[\begin{pmatrix} g_1^{[j]} & \cdots & g_n^{[j]} \\ \vdots & \ddots & \vdots \\ g_1^{[k-2+j]} & \cdots & g_n^{[k-2+j]} \end{pmatrix} - \begin{pmatrix} g_1^{[j]} & \cdots & g_n^{[j]} \\ \vdots & \ddots & \vdots \\ g_1^{[k-2+j]} & \cdots & g_n^{[k-2+j]} \end{pmatrix} \right] = 0_{(k-1)\times n}$$

Tým sme dokázali, že matica $Y_R = \Lambda_{u-1}(Y)$ naozaj spĺňuje (3.2), *pretože sme ju dostali nejakými riadkovými úpravami matice $G_R^{\mathcal{V}}$ v procese eliminácie posledných*

$u(k-1)$ *riadkov* G_R.

□

Ďalej sa pozrieme, čo platí pre riešenie $\mathbf{u} \in \mathbb{F}_{q^m}^{n+t}$ homogénnej sústavy

$$\tilde{G}_R^{\mathcal{V}} \cdot \mathbf{u}^\top = \tilde{S}_R \cdot \begin{bmatrix} Z & G_{n-1} \\ Y_R & 0_{u(k-1)\times n} \end{bmatrix} \cdot T \cdot \mathbf{u}^\top = \mathbf{o}. \tag{3.3}$$

Vektor $T \cdot \mathbf{u}^\top$ môžeme vyjadriť ako $T \cdot \mathbf{u}^\top = \begin{bmatrix} \mathbf{y} & \mathbf{h} \end{bmatrix}^\top$, kde $\mathbf{y} \in \mathbb{F}_{q^m}^t$ a $\mathbf{h} \in \mathbb{F}_{q^m}^n$. Potom homogénna sústava (3.3) je ekvivalentná so sústavou rovníc

$$\begin{aligned} Z \cdot \mathbf{y}^\top + G_{n-1} \cdot \mathbf{h}^\top &= \mathbf{o}, \\ Y_R \cdot \mathbf{y}^\top &= \mathbf{o}. \end{aligned} \tag{3.4}$$

Teraz predpokladajme, že platí $\operatorname{rank}(Y_R) = t$. Potom druhá rovnica v (3.4) má iba triviálne riešenie $\mathbf{y}^\top = \mathbf{o}$. Z toho ale plynie, že v prvej rovnici v (3.4) je iba $G_{n-1} \cdot \mathbf{h}^\top = \mathbf{o}$. Pripomeňme, že matica G_{n-1} je generujúcou maticou Gabidulinovho $[n, n-1]_{q^m}$-kódu. Pretože $n-(n-1) = 1$ a $G_{n-1} \cdot \mathbf{h}^\top = 0$, tak $\mathbf{h}$ je kontrolnou maticou kódu $\langle G_{n-1} \rangle$. Podľa 3. bodu tvrdenia 20 je $\langle G_{n-1} \rangle^\perp$ Gabidulinov $[n, 1]_{q^m}$-kód, ktorý je zrejme generovaný $\mathbf{h}$. Potom z definície Gabidulinovho kódu je $\operatorname{rk}(\mathbf{h}) = n$. Zároveň sme dostali, že $\mathbf{u} = \begin{bmatrix} \mathbf{o} & \mathbf{h} \end{bmatrix} \cdot (T^{-1})^\top \in \mathbb{F}_{q^m}^{n+t}$ je kontrolnou maticou kódu generovaného $G_R^{\mathcal{V}}$, a teda $\mathbf{u}$ generuje jeho duálny kód. Ukážeme, že nutne aj $\operatorname{rk}(\mathbf{u}) = n$.

Uvážme nejakú bázu α telesa $\mathbb{F}_{q^m}$ nad $\mathbb{F}_q$ a označme $T^{-1} = (d_{ij})_{i,j=1}^{n+t}$ pre nejaké $d_{ij} \in \mathbb{F}_q$. Potom môžeme vektor $\mathbf{u}$ vyjadriť pomocou maticového násobenia nad telesom $\mathbb{F}_q$ nasledovne

$$\begin{aligned} U = ([u_1]_\alpha \mid \cdots \mid [u_{n+t}]_\alpha) &= ([0]_\alpha \mid \cdots \mid [0]_\alpha \mid [h_1]_\alpha \mid \cdots \mid [h_n]_\alpha) \cdot (T^{-1})^\top \\ &= \left(\left[\sum_{i=t+1}^{n+t} h_{i-t} d_{1i} \right]_\alpha \,\middle|\, \cdots \,\middle|\, \left[\sum_{i=t+1}^{n+t} h_{i-t} d_{(n+t)i} \right]_\alpha \right) \\ &= \left(\sum_{i=t+1}^{n+t} d_{1i} \, [h_{i-t}]_\alpha \,\middle|\, \cdots \,\middle|\, \sum_{i=t+1}^{n+t} d_{(n+t)i} \, [h_{i-t}]_\alpha \right) \end{aligned} \tag{3.5}$$

Vidíme, že $\operatorname{rk}(\mathbf{u}) = \operatorname{rank}(U) = \operatorname{rank}(([h_1]_\alpha \mid \cdots \mid [h_n]_\alpha)) = n$, keďže násobenie regulárnou maticou nemení hodnosť.

Teraz si v dvoch krokoch ukážeme, ako Overbeckovým útokom z verejného kľúča $\mathcal{K}_{\mathcal{V}} = (G^{\mathcal{V}}, e)$ skonštruujeme nový platný súkromný kľúč za predpokladu, že v (3.2) je $\operatorname{rank}(Y_R) = t$.

3.1.1 Alternatívny kódovač stĺpcov

Pripomeňme, že poznáme maticu $G^{\mathcal{V}} = S \cdot \begin{bmatrix} X & G \end{bmatrix} \cdot T$ a z nej vypočítame maticu $G_R^{\mathcal{V}} = \Lambda_{n-k-1}(G^{\mathcal{V}}) = \left[(G^{\mathcal{V}})^{([i])} \right]_{i=0}^{n-k-1}$. Začneme nájdením alternatívnej regulárnej matice $T_F \in \mathbb{F}_q^{(n+t)\times(n+t)}$, ktorá kóduje stĺpce matice G v $G^{\mathcal{V}}$. Predvedieme konštrukciu matice T_F z $\mathbf{u} = \langle G_R^{\mathcal{V}} \rangle^\perp$ (tj. $\operatorname{LO}(\mathbf{u}) = \ker(G_R^{\mathcal{V}})$) tak, aby platilo $\mathbf{u} = \begin{bmatrix} \mathbf{o} & \mathbf{h} \end{bmatrix} \cdot (T_F^{-1})^\top$ pre nejaké $\mathbf{h} \in \mathbb{F}_{q^m}^n$, $\operatorname{rk}(\mathbf{h}) = n$. Vidíme, že pri konštrukcii

T_F máme určitú slobodu voľby $\mathbf{h}$, avšak získaný Gabidulinov kód bude závisieť na učinenej voľbe.

Zvoľme množinu indexov $I \subset \{1, \ldots, n+t\}$ spĺňajúcu $|I| = n$ a $\mathrm{rk}(\mathbf{u}_I) = n$. Ďalej označme množinu $J = \{1, \ldots, n+t\} \setminus I$ a vektor $\tilde{\mathbf{h}} = \mathbf{u}_I$. Definujme zobrazenie $\pi_J : J \to \mathbb{N}$, ktoré prvku $j \in J$ priradí jeho pozíciu pri vzostupnom usporiadaní množiny. V (3.5) sme ukázali, že $\mathrm{rk}(\mathbf{u}) = n = \mathrm{rk}(\tilde{\mathbf{h}})$, takže zvyšných t prvkov $\mathbf{u}$ (tj. $\mathbf{u}_J$) musí byť $\mathbb{F}_q$-lineárnou kombináciou zložiek $\tilde{\mathbf{h}}$. Inými slovami, existuje matica $\tilde{T} = (\tilde{t}_{ij}) \in \mathbb{F}_q^{n \times t}$ spĺňajúca $\mathbf{u}_J = \tilde{\mathbf{h}} \cdot \tilde{T}$, z čoho môžeme pre každé $j \in J$ vyjadriť $u_j = \sum_{i=1}^{n} \tilde{h}_i \tilde{t}_{i\pi_J(j)}$. Chceme nájsť regulárnu maticu T_F tak, aby $\mathbf{u} = \begin{bmatrix} \mathbf{o} & \tilde{\mathbf{h}} \end{bmatrix} \cdot (T_F^{-1})^\top$. Označme prvky $T_F^{-1} = (d_{ij})_{i,j=1}^{n+t}$ a vyjadrime si, čo pre ne platí:

$$
\begin{aligned}
u_j = \sum_{i=1}^{n} \tilde{h}_i \cdot d_{j(i+t)} &= \begin{cases} \tilde{h}_{\pi_I(j)} & \text{ak } j \in I \\ \sum_{i=1}^{n} \tilde{h}_i \cdot \tilde{t}_{i\pi_J(j)} & \text{ak } j \in J \end{cases} \\
\overset{\text{volíme}}{\Longrightarrow} d_{ji} &= \begin{cases} 1 & \text{ak } j \in J, i = \pi_J(j), \text{ alebo } j \in I, i = \pi_I(j) + t \\ \tilde{t}_{(i-t)\pi_J(j)} & \text{ak } j \in J \text{ a } i > t \\ 0 & \text{inak} \end{cases}
\end{aligned}
\tag{3.6}
$$

Pre prehľadnosť a lepšie pochopenie, ako sme volili prvky d_{ji} v (3.6), vyjadríme T_F^{-1} maticovým násobením ako $T_F^{-1} = P \cdot \begin{bmatrix} I_t & \tilde{T}^\top \\ 0_{n \times t} & I_n \end{bmatrix}$, kde $P \in \mathbb{F}_q^{(n+t)\times(n+t)}$ je vhodne zvolená permutačná matica. Zároveň priamo vidíme, že T_F^{-1} je súčin dvoch regulárnych matíc nad $\mathbb{F}_q$, z čoho plynie, že je to regulárna matica. Teda naozaj existuje $T_F = (T_F^{-1})^{-1} \in \mathbb{F}_q^{(n+t)\times(n+t)}$.

3.1.2 Alternatívny Gabidulinov kód

Poznamenajme, že už poznáme $\mathbf{u}, \tilde{\mathbf{h}}$ a maticu T_F. Teraz sa zameriame na hľadanie matice $G_F \in \mathbb{F}_{q^m}^{k \times n}$ generujúcej Gabidulinov $[n,k]_{q^m}$-kód, ktorého kontrolná matica je generovaná vektorom $\tilde{\mathbf{h}}$. Vyjadrime si, čo platí pre riešenie homogénnej sústavy s $G_R^{\mathcal{V}}$:

$$
\begin{aligned}
& G_R^{\mathcal{V}} \cdot \mathbf{u}^\top = \mathbf{o} \iff G_R^{\mathcal{V}} \cdot T_F^{-1} \cdot \begin{bmatrix} \mathbf{o} \\ \tilde{\mathbf{h}}^\top \end{bmatrix} = \mathbf{o} \\
& \overset{(T_F^{-1})^{([i])} = T_F^{-1}}{\iff} \begin{bmatrix} G^{\mathcal{V}} \cdot T_F^{-1} \\ (G^{\mathcal{V}} \cdot T_F^{-1})^{([1])} \\ \vdots \\ (G^{\mathcal{V}} \cdot T_F^{-1})^{([n-k-1])} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{o} \\ \tilde{\mathbf{h}}^\top \end{bmatrix} = \mathbf{o} \\
& \iff (G^{\mathcal{V}} \cdot T_F^{-1})^{([i])} \cdot \begin{bmatrix} \mathbf{o} \\ \tilde{\mathbf{h}}^\top \end{bmatrix} = \mathbf{o} \quad \forall\, i = 0, \ldots, n-k-1 \\
& \iff (G^{\mathcal{V}} \cdot T_F^{-1}) \cdot \begin{bmatrix} \mathbf{o} \\ \tilde{\mathbf{h}}^\top \end{bmatrix}^{([-i])} = \mathbf{o} \quad \forall\, i = 0, \ldots, n-k-1
\end{aligned}
\tag{3.7}
$$

Označme bloky $G^{\mathcal{V}} \cdot T_F^{-1} = \begin{bmatrix} X_F & G_F \end{bmatrix}$ a položme $H_F = \left(\tilde{\mathbf{h}}^{([i-n+k])}\right)_{i=1}^{n-k} \in \mathbb{F}_{q^m}^{(n-k)\times n}$. Potom zo sústavy ekvivalentných rovníc (3.7) plynie:

$$G_F \cdot H_F^{\top} = 0_{k\times(n-k)} \tag{3.8}$$

Pretože $\mathrm{rk}(\tilde{\mathbf{h}}) = n$ z voľby $\tilde{\mathbf{h}}$, tak matica H_F je generujúcou maticou Gabidulinovho $[n, n-k]_{q^m}$-kódu. Teda podľa tvrdenia 20.3 je H_F kontrolnou maticou Gabidulinovho $[n,k]_{q^m}$-kódu. Odtiaľto a z rovnosti (3.8) už dostávame, že riadky matice $G_F \in \mathbb{F}_{q^m}^{k\times n}$ generujú Gabidulinov $[n,k]_{q^m}$-kód (G_F nemusí byť v tvare $G_F = (\tilde{\mathbf{g}}^{([i-1])})_{i=1}^{k}$).

Poznámka. Existujú matice $S_F \in \mathbb{F}_{q^m}^{k\times k}, \mathrm{rank}(S_F) = k$, a $\tilde{G} = \left(\tilde{\mathbf{g}}^{([i-1])}\right)_{i=1}^{k} \in \mathbb{F}_{q^m}^{k\times n}$, $\mathrm{rk}(\tilde{\mathbf{g}}) = n$, splňujúce $S_F \cdot \tilde{G} = G_F$, pretože elementárne riadkové úpravy nemenia riadkový priestor matice.

Lemma 33. *Nech $\mathcal{K}_{\mathcal{S}} = (\mathcal{D}_{\mathcal{G}}, G, S, T)$ je súkromný kľúč GPT kryptosystému a $\mathcal{K}_{\mathcal{V}} = (G^{\mathcal{V}}, e)$ je príslušný verejný kľúč. Označme $\mathcal{K}_{\mathcal{S}}^{\mathcal{F}} = (\mathcal{D}_{\langle G_F\rangle}, G_F, T_F)$ súkromný kľúč získaný Overbeckovým útokom za predpokladu, že je útok možný. Potom $\mathcal{K}_{\mathcal{S}}^{\mathcal{F}}$ dešifruje správy šifrované verejným kľúčom $\mathcal{K}_{\mathcal{V}}$.*

Dôkaz. Nech $\mathbf{c} \in \mathbb{F}_{q^m}^{n+t}$ je zašifrovaná správa, teda existujú správa $\mathbf{x} \in \mathbb{F}_{q^m}^{k}$ a vektor chyby $z \in \mathbb{F}_{q^m}^{n+t}, \mathrm{rk}(\mathbf{z}) \le e$, také, že $\mathbf{c} = \mathbf{x}\cdot G^{\mathcal{V}} + \mathbf{z}$. Označme $I = \{t+1, \ldots, n+t\}$ indexy posledných n stĺpcov matice $G^{\mathcal{V}}$. Pripomeňme, že $G^{\mathcal{V}} \cdot T_F^{-1} \overset{(3.7)}{=} \begin{bmatrix} X_F & G_F \end{bmatrix}$. Postupnými úpravami $\mathbf{c}$ predvedieme, že sme schopní určiť pôvodnú správu $\mathbf{x}$:

$$\begin{aligned} \mathbf{c} &= \mathbf{x}\cdot G^{\mathcal{V}} + \mathbf{z} \\ \mathbf{c}\cdot T_F^{-1} &= \mathbf{x}\cdot G^{\mathcal{V}}\cdot T_F^{-1} + \mathbf{z}\cdot T_F^{-1} \\ \underbrace{(\mathbf{c}\cdot T_F^{-1})_I}_{\tilde{\mathbf{c}}} &= \mathbf{x}\cdot (G^{\mathcal{V}}\cdot T_F^{-1})_{.I} + (\mathbf{z}\cdot T_F^{-1})_I \\ \mathcal{D}_{\langle G_F\rangle}(\tilde{\mathbf{c}}) &= \mathbf{x}\cdot (G^{\mathcal{V}}\cdot T_F^{-1})_{.I} = \mathbf{x}\cdot G_F \end{aligned}$$

Využili sme, že $\mathrm{rk}((\mathbf{z}\cdot T_F^{-1})_I) \le \mathrm{rk}(\mathbf{z}\cdot T_F^{-1}) = \mathrm{rk}(\mathbf{z}) \le e$, keďže násobenie regulárnou maticou nemení hodnosť. Takže $\mathbf{x} \in \mathbb{F}_{q^m}^{k}$ získame ako riešenie sústavy lineárnych rovníc $\mathbf{x}\cdot G_F = \mathcal{D}_{\langle G_F\rangle}(\tilde{\mathbf{c}})$ nad telesom $\mathbb{F}_{q^m}$, kde existencia a jednoznačnosť riešenia plynie z rovnosti $G_F = (G^{\mathcal{V}}\cdot T_F^{-1})_{.I} = \left(S\cdot\begin{bmatrix} X & G \end{bmatrix}\cdot T\cdot T_F^{-1}\right)_{.I}$. Tým sme dokázali, že $\mathcal{K}_{\mathcal{S}}^{\mathcal{F}}$ je alternatívny súkromný kľúč k verejnému kľúču $\mathcal{K}_{\mathcal{V}}$.

□

Dôsledok (Overbeck a kol., 2005, Veta 3). Ak má matica Y_R v (3.2) hodnosť t, tak potom Overbeckov útok prelomí GPT kryptosystém v čase $O\left((n+t)^3\right)$ (operácie nad $\mathbb{F}_{q^m}$).

Keďže sme už popísali celý Overbeckov útok na GPT kryptosystém a i dokázali, že naozaj funguje, tak nám ešte zostáva si útok ilustrovať na príklade.

Príklad. Majme $q = 2, m = n = 5$ a $k = t = 2$. Nech $B = (1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ je báza telesa $\mathbb{F}_{2^5}$ nad $\mathbb{F}_2$, v ktorom budeme počítať modulo ireducibilný polynóm $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$. Prvok $a = \sum_{i=0}^{4} a_i \cdot \alpha^i \in \mathbb{F}_{2^5}$ budeme zapisovať

ako $a_4a_3a_2a_1a_0$. Majme $\mathbf{g} = (10100,01001,00111,10110,11001) \in \mathbb{F}_{2^5}$ generujúci vektor, overíme jeho hodnosť:

$$[\mathbf{g}]_B = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \implies \mathrm{rk}(\mathbf{g}) = 5.$$

Potom $G = \begin{pmatrix} \mathbf{g} \\ \mathbf{g}^{(2)} \end{pmatrix} = \begin{pmatrix} 10100 & 01001 & 00111 & 10110 & 11001 \\ 11101 & 01011 & 10101 & 11001 & 00110 \end{pmatrix}$ je generujúca matica Gabidulinoveho $[5,2]_{2^5}$-kódu $\mathcal{G}$, ktorý opraví $\lfloor \frac{5-2}{2} \rfloor = 1$ chybu. Ďalej nech $X = \begin{pmatrix} 11000 & 00100 \\ 01000 & 00010 \end{pmatrix}$, $S = \begin{pmatrix} 00010 & 00101 \\ 00001 & 01100 \end{pmatrix} \in \mathbb{F}_{2^5}^{2\times 2}$ a $T = \begin{pmatrix} 0&0&1&0&1&1&0 \\ 1&1&0&0&0&1&0 \\ 1&0&1&0&1&0&1 \\ 0&1&0&1&1&1&0 \\ 0&1&1&0&0&1&0 \\ 0&0&0&0&0&1&1 \\ 0&0&0&1&0&1&1 \end{pmatrix} \in \mathbb{F}_2^{7\times 7}$.

Potom verejná matica je

$$G^{\mathcal{V}} = S \begin{bmatrix} X & G \end{bmatrix} \cdot T = \begin{pmatrix} 01001 & 10111 & 10110 & 11001 & 00011 & 11101 & 11001 \\ 00000 & 01110 & 01011 & 00110 & 11001 & 00110 & 00011 \end{pmatrix}.$$

Označme $\mathcal{K}_{\mathcal{V}} = (G^{\mathcal{V}},1)$ verejný kľúč a $\mathcal{K}_{\mathcal{S}} = (\mathcal{D}_{\mathcal{G}}, G, S, T)$ súkromný kľúč. Nech

$\mathbf{m} = (00010,01101)$ je správa,
$\mathbf{z} = (00011,00000,00011,00000,00000,00011,00000), \mathrm{rk}(\mathbf{z}) = 1,$ vektor chyby,
$\mathbf{c} = \mathbf{x} \cdot G^{\mathcal{V}} + z = (10001,00111,11010,11100,00010,10111,00000)$

je šifrový text.

Z pohľadu útočníka na GPT kryptosystém poznáme iba $\mathcal{K}_{\mathcal{V}}$ a prípadne zachytenú komunikáciu, ktorú reprezentuje $\mathbf{c}$. Rovno prejdime k útoku s parametrom $u = n - k - 1 = 5 - 2 - 1 = 2$:

$$G_R^{\mathcal{V}} = \Lambda_u(G^{\mathcal{V}}) = [(G^{\mathcal{V}})^{([i])}]_{i=0}^{2} = \begin{pmatrix} 01001 & 10111 & 10110 & 11001 & 00011 & 11101 & 11001 \\ 00000 & 01110 & 01011 & 00110 & 11001 & 00110 & 00011 \\ 01011 & 11000 & 11001 & 00110 & 00101 & 10110 & 00110 \\ 00000 & 11110 & 01111 & 10100 & 00110 & 10100 & 00101 \\ 01111 & 00111 & 00110 & 10100 & 10001 & 11001 & 10100 \\ 00000 & 10011 & 11111 & 11101 & 10100 & 11101 & 10001 \end{pmatrix}$$

$$\sim \begin{pmatrix} 00001 & 10110 & 10010 & 01011 & 01100 & 11011 & 01011 \\ 00000 & 00001 & 11111 & 10100 & 11100 & 10100 & 01010 \\ 00000 & 00000 & 00001 & 00101 & 11001 & 10000 & 11011 \\ 00000 & 00000 & 00000 & 00001 & 00010 & 01100 & 00011 \\ 00000 & 00000 & 00000 & 00000 & 00001 & 01001 & 00000 \\ 00000 & 00000 & 00000 & 00000 & 00000 & 00001 & 11101 \end{pmatrix}$$

$$\implies \mathrm{rank}(G_R^{\mathcal{V}}) = 6 = \underbrace{\mathrm{rank}\left(\left(\mathbf{g}^{([i-1])}\right)_{i=1}^{4}\right)}_{4} + 2,$$

takže Overbeckov útok sa dá použiť na prelomenie GPT kryptosystému s danými parametrami. Teraz určíme $\ker(G_R^{\mathcal{V}})$ a zvolíme nejaké $\mathbf{u}^\top \in \ker(G_R^{\mathcal{V}})$:

$$\begin{aligned}
u_7 &= a \in \mathbb{F}_{2^5} \\
u_6 &= 11101 \cdot u_7 = 11101 \cdot a \\
u_5 &= 01001 \cdot u_6 = 01110 \cdot a \\
u_4 &= 00010 \cdot u_5 + 01100 \cdot u_6 + 00011 \cdot u_7 = 10111 \cdot a \\
u_3 &= 00101 \cdot u_4 + 11001 \cdot u_5 + 10000 \cdot u_6 + 11011 \cdot u_7 = 10011 \cdot a \\
u_2 &= 11111 \cdot u_3 + 10100 \cdot u_4 + 11100 \cdot u_5 + 10100 \cdot u_6 + 01010 \cdot u_7 = 01101 \cdot a \\
u_1 &= 10110 \cdot u_2 + 10010 \cdot u_3 + 01011 \cdot u_4 + 01100 \cdot u_5 + 11011 \cdot u_6 + 01011 \cdot u_7 \\
&= 10000 \cdot a
\end{aligned}$$

$$\implies \ker(G_R^{\mathcal{V}}) = \left\{ \begin{pmatrix} 10000\cdot a \\ 01101\cdot a \\ 10011\cdot a \\ 10111\cdot a \\ 01110\cdot a \\ 11101\cdot a \\ a \end{pmatrix} \;\middle|\; a \in \mathbb{F}_{2^5} \right\} \overset{a=00010}{\implies} \mathbf{u}^\top = \begin{pmatrix} 00101 \\ 11010 \\ 00011 \\ 01011 \\ 11100 \\ 11111 \\ 00010 \end{pmatrix}$$

Označme množinu indexov $I = \{2,3,4,5,7\}$ a $J = \{1,6\}$. Overíme, že $\mathrm{rk}(\mathbf{u}_I) = 5$:

$$[\mathbf{u}_I]_B = \begin{pmatrix} 0\,1\,1\,0\,0 \\ 1\,1\,1\,0\,1 \\ 0\,0\,0\,1\,0 \\ 1\,0\,1\,1\,0 \\ 1\,0\,0\,1\,0 \end{pmatrix} \sim \begin{pmatrix} 1\,0\,0\,1\,0 \\ 0\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0 \\ 0\,0\,0\,1\,0 \\ 0\,0\,0\,0\,1 \end{pmatrix} \implies \mathrm{rank}([\mathbf{u}_I]_B) = 5$$

Takže môžeme položiť $\tilde{\mathbf{h}} = \mathbf{u}_I$. Určíme maticu $\tilde{T} \in \mathbb{F}_2^{2\times 5}$ takú, že pre ňu platí $\tilde{\mathbf{h}} \cdot \tilde{T}^\top = \mathbf{u}_J = (00101, 11111)$. To splňuje napríklad $\tilde{T} = \left(\begin{smallmatrix} 1\,1\,0\,1\,0 \\ 0\,1\,0\,1\,0 \end{smallmatrix}\right)$. Takže už môžeme zostrojiť $T_F \in \mathbb{F}_2^{7\times 7}, \mathrm{rank}(T_F) = 7$, tak, aby:

$$T_F^{-1} = P \cdot \left(\begin{smallmatrix} I_2 & \tilde{T} \\ 0_{5\times 2} & I_5 \end{smallmatrix}\right) = \begin{pmatrix} 1\,0\,1\,1\,0\,1\,0 \\ 0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0 \\ 0\,1\,0\,1\,0\,1\,0 \\ 0\,0\,0\,0\,0\,0\,1 \end{pmatrix}, \text{ kde } P = \begin{pmatrix} 1\,0\,0\,0\,0\,0\,0 \\ 0\,0\,1\,0\,0\,0\,0 \\ 0\,0\,0\,1\,0\,0\,0 \\ 0\,0\,0\,0\,1\,0\,0 \\ 0\,0\,0\,0\,0\,1\,0 \\ 0\,1\,0\,0\,0\,0\,0 \\ 0\,0\,0\,0\,0\,0\,1 \end{pmatrix} \in \mathbb{F}_2^{7\times 7}$$

je permutačná matica. Potom naozaj platí $\mathbf{u} = (00000, 00000, \tilde{\mathbf{h}}) \cdot (\tilde{T}_F^{-1})^\top$. Konečne môžeme určiť maticu $G_F \in \mathbb{F}_{2^5}^{2\times 5}$, ktorej riadky generujú Gabidulinov $[5,2]_{2^5}$-kód $\mathcal{G}_{\mathcal{F}}$ s kontrolnou maticou $H_F = \left(\tilde{\mathbf{h}}^{([i-2])}\right)_{i=0}^{2} = \left(\begin{smallmatrix} 10001\ 01100\ 10010\ 00111\ 01101 \\ 01100\ 11010\ 01001\ 10101\ 11011 \\ 11010\ 00011\ 01011\ 11100\ 00010 \end{smallmatrix}\right)$:

$$G^{\mathcal{V}} \cdot T_F^{-1} = \Big(\underbrace{\begin{smallmatrix} 01001\ 11101 \\ 00000\ 00110 \end{smallmatrix}}_{X_F} \underbrace{\begin{smallmatrix} 11110\ 00010\ 11001\ 10111\ 11001 \\ 01110\ 01101\ 00110\ 11111\ 00011 \end{smallmatrix}}_{G_F} \Big).$$

Ľahko overíme, že

$$G_F \cdot H_F^\top = \left(\begin{smallmatrix} 11110\ 00010\ 11001\ 10111\ 11001 \\ 01110\ 01101\ 00110\ 11111\ 00011 \end{smallmatrix}\right) \cdot \begin{pmatrix} 10001\ 01100\ 11010 \\ 01100\ 11010\ 00011 \\ 10010\ 01001\ 01011 \\ 00111\ 10101\ 11100 \\ 01101\ 11011\ 00010 \end{pmatrix} = \left(\begin{smallmatrix} 00000\ 00000\ 00000 \\ 00000\ 00000\ 00000 \end{smallmatrix}\right).$$

Na záver zostáva overiť, či sme schopní dešifrovať správu $\mathbf{c}$, pričom dekódovací algoritmus $\mathcal{D}_{\mathcal{G}_{\mathcal{F}}}$ budeme simulovať odčítaním vektoru chyby $(\mathbf{z} \cdot T_F^{-1})_{\{3,\ldots,7\}}$ (vektor chyby útočník nepozná):

$$\begin{aligned}
\mathbf{c}' &= \mathbf{c} \cdot T_F^{-1} = \left(\begin{smallmatrix} 10001\ 10111\ 10110\ 11100\ 11100\ 00100\ 00000 \end{smallmatrix}\right) \\
\mathbf{z}' &= \mathbf{z} \cdot T_F^{-1} = \left(\begin{smallmatrix} 00011\ 00011\ 00011\ 00011\ 00000\ 00000\ 00000 \end{smallmatrix}\right) \\
\mathbf{y} &= \mathcal{D}_{\mathcal{G}_{\mathcal{F}}}(\mathbf{c}'_{\{3,\ldots,7\}}) = \mathbf{c}'_{\{3,\ldots,7\}} - \mathbf{z}'_{\{3,\ldots,7\}} = \left(\begin{smallmatrix} 10101\ 11111\ 11100\ 00100\ 00000 \end{smallmatrix}\right) \\
&\implies \left(G_F^\top \;\middle|\; \mathbf{y}^\top\right) = \left(\begin{smallmatrix} 11110\ 01110 & 10101 \\ 00010\ 01101 & 11111 \\ 11001\ 00110 & 11100 \\ 10111\ 11111 & 00100 \\ 11001\ 00011 & 00000 \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} 00001\ 00110 & 01001 \\ 00000\ 00001 & 01101 \\ 00000\ 00000 & 00000 \\ 00000\ 00000 & 00000 \\ 00000\ 00000 & 00000 \end{smallmatrix}\right) \\
&\implies \text{riešenie sústavy je } x_2 = 01101 \text{ a } x_1 = 00110 \cdot x_2 + 01001 = 00010
\end{aligned}$$

Dostali sme teda $\mathbf{x} = (x_1, x_2) = (00010, 01101) = \mathbf{m}$, čo je dôkaz o prelomení bezpečnosti komunikácie šifrovanej verejným kľúčom $\mathcal{K}_{\mathcal{V}}$.

Všetky výpočty boli robené v programe Wolfram Mathematica verzia 12.1, pričom kód k tomuto príkladu je priložený ako príloha A.1.

Príklad. Majme GPT kryptosystém s rovnakými parametrami ako v predošlom príklade až na maticu X, ktorú zadefinujeme neskôr. Teda máme dané parametre $q = 2, m = n = 5$ a $k = t = 2$, teleso $\mathbb{F}_{2^5}$, v ktorom počítame modulo ireducibilný polynóm $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ a Gabidulinov $[5,2]_{2^5}$-kód generovaný

vektorom $\mathbf{g} = (10100,01001,00111,10110,11001) \in \mathbb{F}_{2^5}$. Pripomeňme matice z predošlého príkladu a rovno i definujme novú maticu X:

$$G = \begin{pmatrix} \mathbf{g} \\ \mathbf{g}^{(2)} \end{pmatrix} = \begin{pmatrix} 10100 & 01001 & 00111 & 10110 & 11001 \\ 11101 & 01011 & 10101 & 11001 & 00110 \end{pmatrix} \in \mathbb{F}_{2^5}^{2\times 5},$$
$$X = \begin{pmatrix} 00010 & 00011 \\ 00101 & 00100 \end{pmatrix}, S = \begin{pmatrix} 00010 & 00101 \\ 00001 & 01100 \end{pmatrix} \in \mathbb{F}_{2^5}^{2\times 2},$$
$$T = \begin{pmatrix} 0&0&1&0&1&1&0 \\ 1&1&0&0&0&1&0 \\ 1&0&1&0&1&0&1 \\ 0&1&0&1&1&1&0 \\ 0&1&1&0&0&1&0 \\ 0&0&0&0&0&1&1 \\ 0&0&0&1&0&1&1 \end{pmatrix} \in \mathbb{F}_2^{7\times 7}.$$

Potom verejná matica je

$$G^{\mathcal{V}} = S \begin{bmatrix} X & G \end{bmatrix} \cdot T = \left(\begin{smallmatrix} 11001 & 00111 & 11011 & 11001 & 01110 & 00000 & 11001 \\ 01010 & 00100 & 00111 & 00110 & 10101 & 00000 & 00011 \end{smallmatrix} \right).$$

Rovno určime rozšírenú verejnú maticu s parametrom $u = n - k - 1 = 2$:

$$G_R^{\mathcal{V}} = \Lambda_u(G^{\mathcal{V}}) = [(G^{\mathcal{V}})^{([i])}]_{i=0}^{2} = \begin{pmatrix} 11001 & 00111 & 11011 & 11001 & 01110 & 00000 & 11001 \\ 01010 & 00100 & 00111 & 00110 & 10101 & 00000 & 00011 \\ 00110 & 10101 & 00010 & 00110 & 11110 & 00000 & 00110 \\ 01110 & 10000 & 10101 & 10100 & 11100 & 00000 & 00101 \\ 10100 & 11100 & 00100 & 10100 & 10011 & 00000 & 10100 \\ 11110 & 01101 & 11100 & 11101 & 10111 & 00000 & 10001 \end{pmatrix}$$
$$\sim \begin{pmatrix} 00001 & 10011 & 10101 & 00001 & 00011 & 00000 & 00001 \\ 00000 & 00001 & 11101 & 11110 & 00001 & 00000 & 00100 \\ 00000 & 00000 & 00001 & 11110 & 01001 & 00000 & 00100 \\ 00000 & 00000 & 00000 & 00001 & 11001 & 00000 & 11101 \\ 00000 & 00000 & 00000 & 00000 & 00001 & 00000 & 01110 \\ 00000 & 00000 & 00000 & 00000 & 00000 & 00000 & 00000 \end{pmatrix}$$
$$\implies \operatorname{rank}(G_R^{\mathcal{V}}) = 5 = \underbrace{\operatorname{rank}\left(\left(\mathbf{g}^{([i-1])}\right)_{i=1}^{4}\right)}_{4} + 1.$$

Pretože $\operatorname{rank}(G_R^{\mathcal{V}}) = 5 < \operatorname{rank}\left(\left(\mathbf{g}^{([i-1])}\right)_{i=1}^{4}\right) + t = 4 + 2 = 6$, tak rovnica $Y_R \cdot \mathbf{y}^\top = \mathbf{o}$ v (3.4) má netriviálne riešenie. Potom ale nemôžeme člen $Z \cdot \mathbf{y}^\top$ z rovnice $Z \cdot \mathbf{y}^\top + G_{n-1} \cdot \mathbf{h}^\top = \mathbf{o}$ v (3.4) vynechať. Preto nemôžeme previesť Overbeckov útok na získanie $\mathbf{h}$ v $T \cdot \mathbf{u}^\top = \begin{bmatrix} \mathbf{y} & \mathbf{h} \end{bmatrix}^\top$ z lineárnej sústavy (3.4).

3.2 Obrana proti Overbeckovmu útoku

Ako sme ukázali v predošlom príklade, tak existujú voľby matice X, pre ktoré sa Overbeckov útok nedá použiť. V tejto podkapitole si ukážeme poznatky z 5. kapitoly článku Rashwan a kol. (2010), konkrétne ako presne sa tieto matice dajú skonštruovať a na čo si dať pri voľbe X pozor. Základnou ideou je zvoliť maticu X tak, aby pre príšlusnú maticu Y_R platilo $\operatorname{rank}(Y_R) = t - a$, kde $a \geq 2$. Potom druhá rovnica v sústave (3.4) má $q^{a \cdot m}$ možných riešení $\mathbf{y}^\top$. Z tohto dôvodu je teda nutné skúšať všetky platné možnosti $\mathbf{y}^\top$, čo znamená, že pre hľadanie vektoru $\mathbf{h}$ kontrolnej matice potrebujeme $O(q^{a \cdot m}(n+t)^3)$ operácií nad telesom $\mathbb{F}_q$. V celej tejto podkapitole budeme bez ujmy na všeobecnosti pracovať s maticou Y_R v tvare z lemmy 32.

Lemma 34. *Nech $s \in \mathbb{N}$. Ak má matica Y hodnosť $\operatorname{rank}_q^{\downarrow}(Y) = s$, tak potom aj Y_R má hodnosť $\operatorname{rank}_q^{\downarrow}(Y_R) = s$.*

Dôkaz. Tvrdenie triviálne platí, pretože matica Y_R vznikla z matice Y pridávaním riadkov matice Y umocnených po prvku na $[i]$ pre $1 \leq i \leq u-1$. Teda stĺpce Y_R dostaneme prostým $\mathbb{F}_q$-lineárnym zobrazením stĺpcov Y, čiže sa zachováva lineárna závislosť stĺpcov.

□

Dôsledok. Platí $\operatorname{rank}(Y_R) = \operatorname{rank}^{|}_{q^m}(Y_R) \leq \operatorname{rank}^{|}_{q}(Y_R) = \operatorname{rank}^{|}_{q}(Y)$.

Najprv predpokladajme, že matica X je v špeciálnom tvare

$$X = \begin{pmatrix} \mathbf{m} \\ \mathbf{m}^{([1])} \\ \vdots \\ \mathbf{m}^{([k-1])} \end{pmatrix} + \begin{pmatrix} \mathbf{o} \\ \mathbf{s_1} \\ \vdots \\ \mathbf{s}_{k-1} \end{pmatrix}, \text{ kde } \mathbf{m} \in \mathbb{F}_{q^m}^t, \operatorname{rk}(\mathbf{m}) = t, \mathbf{s_1}, \ldots, \mathbf{s}_{k-1} \in \mathbb{F}_q^t,$$

pre ktoré platí, že $\operatorname{rank}\left(\begin{pmatrix}\mathbf{o}^\top & \mathbf{s_1}^\top & \ldots & \mathbf{s}_{k-1}^\top\end{pmatrix}\right) = t - a, a \geq 2$. Označme X_1 podmaticu X, ktorú sme dostali vynechaním posledného riadku, a X_2 podmaticu X, ktorú sme dostali vynechaním prvého riadku. Potom pre matice $Y = X_1^{([1])} - X_2$ a Y_R z lemmy 32 plati:

$$\begin{aligned} Y = X_1^{([1])} - X_2 &= \begin{pmatrix} \mathbf{m}^{([1])} - (\mathbf{m}^{([1])} + \mathbf{s_1}) \\ (\mathbf{m}^{([1])} + \mathbf{s_1})^{([1])} - (\mathbf{m}^{([2])} + \mathbf{s_2}) \\ \vdots \\ (\mathbf{m}^{([k-2])} + \mathbf{s}_{k-2})^{([1])} - (\mathbf{m}^{([k-1])} + \mathbf{s}_{k-1}) \end{pmatrix} \\ &= \begin{pmatrix} -\mathbf{s_1} \\ \mathbf{s_1}^{([1])} - \mathbf{s_2} \\ \vdots \\ \mathbf{s}_{k-2}^{([1])} - \mathbf{s}_{k-1} \end{pmatrix} = \begin{pmatrix} -\mathbf{s_1} \\ \mathbf{s_1} - \mathbf{s_2} \\ \vdots \\ \mathbf{s}_{k-2} - \mathbf{s}_{k-1} \end{pmatrix} \sim \begin{pmatrix} \mathbf{s_1} \\ \mathbf{s_2} \\ \vdots \\ \mathbf{s}_{k-1} \end{pmatrix}, \\ \implies Y^{([1])} &= \begin{pmatrix} (-\mathbf{s_1})^{([1])} \\ (\mathbf{s_1} - \mathbf{s_2})^{([1])} \\ \vdots \\ (\mathbf{s}_{k-2} - \mathbf{s}_{k-1})^{([1])} \end{pmatrix} = \begin{pmatrix} -\mathbf{s_1} \\ \mathbf{s_1} - \mathbf{s_2} \\ \vdots \\ \mathbf{s}_{k-2} - \mathbf{s}_{k-1} \end{pmatrix} = Y, \\ \implies Y_R = \Lambda_{u-1}(Y) &= \begin{bmatrix} Y \\ Y^{([1])} \\ \vdots \\ Y^{([u-1])} \end{bmatrix} = \begin{bmatrix} Y \\ Y \\ \vdots \\ Y \end{bmatrix}, \end{aligned}$$

kde sme využili, že umocnenie na $[i]$ je $\mathbb{F}_q$-automorfizmus telesa $\mathbb{F}_{q^m}$. Teda sme ukázali, že $\operatorname{rank}(Y_R) = \operatorname{rank}(Y) = t - a$. Takže podľa úvahy na začiatku tejto podkapitoly má Overbeckov útok pre takúto voľbu matíc exponenciálnu zložitosť v a nad $\mathbb{F}_q$.

Poznámka. Ľahko nahliadneme, že matica X v druhom príklade v predošlej podkapitole bola práve v špeciálnom tvare z predpokladu:

$$X = \begin{pmatrix} 00010 & 00011 \\ 00101 & 00100 \end{pmatrix} = \begin{pmatrix} 00010 & 00011 \\ 00010^2 & 00011^2 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

Teraz sa pozrieme, ako vieme voľbu matice X zovšeobecniť, aby sme ju nemuseli hľadať v predošlom špeciálnom tvare.

Definícia 35. *Nech* $k \in \mathbb{N}$ *a* $\mathbf{w} \in \mathbb{F}_{q^m}^k$. *Povieme, že* $\mathbf{w}$ *je* Frobeniov vektor, *ak platí* $\mathbf{w} = (w, w^{[1]}, \ldots, w^{[k-1]})$.

Všimnime si, že ak máme $\mathbf{w} \in \mathbb{F}_{q^m}^k$ Frobeniov vektor, tak potom dostávame $\mathbf{w}_{\{1,\ldots,k-1\}}^{([1])} - \mathbf{w}_{\{2,\ldots,k\}} = \mathbf{o}$. Presne takýmto vzťahom však máme definované stĺpcové vektory matice Y v lemme 32. Takže nám stačí zvoliť maticu $X \in \mathbb{F}_{q^m}^{k\times t}$ tak, aby $a \geq 2$ stĺpcov boli Frobeniove vektory a zvyšných $t-a$ stĺpcov neboli Frobeniove vektory, pričom požadujeme lineárnu nezávislosť všetkých t stĺpcových vektorov. Potom podľa predchádzajúcej úvahy má matica Y aspoň a nulových stĺpcov, teda $\operatorname{rank}_q^{|}(Y) \leq t-a$. Avšak, podľa dôsledku lemmy 34 už priamo dostávame $\operatorname{rank}(Y_R) \leq \operatorname{rank}_q^{|}(Y) \leq t-a$. Tým sme opäť znemožnili preveditelnosť Overbeckovho útoku.

Príklad. V tomto príklade sa pozrieme na možnú voľbu matice X pre parametre $q = 2, m = 5, k = t = 3$ a $a = 2$. Nech $B = (1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ je báza telesa $\mathbb{F}_{2^5}$ nad $\mathbb{F}_2$, v ktorom budeme počítať modulo polynóm $f(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$ ako v predošlých príkladoch. Definujme maticu X nasledovne:

$$X = \begin{pmatrix} \mathbf{x_1} \\ \mathbf{x_2} \\ \mathbf{x_3} \end{pmatrix} = \begin{pmatrix} 00110 & 01000 & 00010 \\ (00110)^{[1]} & (01000)^{[1]} & 00011 \\ (00110)^{[2]} & (01000)^{[2]} & 10000 \end{pmatrix} = \begin{pmatrix} 00110 & 01000 & 00010 \\ 10100 & 01010 & 00011 \\ 11101 & 01110 & 10000 \end{pmatrix}$$
$$\sim \begin{pmatrix} 00110 & 01000 & 00010 \\ 00000 & 11111 & 01111 \\ 00000 & 00111 & 11011 \end{pmatrix} \sim \begin{pmatrix} 00110 & 01000 & 00010 \\ 00000 & 11111 & 01111 \\ 00000 & 00000 & 11101 \end{pmatrix} \implies \operatorname{rank}(X) = 3.$$

Okamžite vidíme, že prvé dva stĺpce matice X sú Frobeniove vektory a tretí stĺpec nie je Frobeniov vektor, pretože napríklad $(00010)^{[1]} = 00100 \neq 00011$. Ďalej si vyjadríme maticu Y a skontrolujeme jej hodnosť:

$$Y = \begin{pmatrix} \mathbf{x_1}^{([1])} - \mathbf{x_2} \\ \mathbf{x_2}^{([1])} - \mathbf{x_3} \end{pmatrix} = \begin{pmatrix} 00000 & 00000 & 00111 \\ 00000 & 00000 & 10101 \end{pmatrix} \implies \operatorname{rank}(Y) = 1 = t - a.$$

Takže zvolená matica X je bezpečná voči Overbeckovmu útoku.

Záver

Cieľom práce bolo skúmať triedu kryptografických systémov založených na samoopravných kódoch využívajúcich hodnostnú metriku namiesto Hammingovej vzdialenosti. V prvej časti práce sme sa preto zamerali na zhrnutie poznatkov z teórie kódov so zameraním na kódy hodnostnej metriky. Našim prínosom pri spracovaní citovaných zdrojov v tejto časti je rozšírenie jednotlivých podkapitol o tvrdenia 2 a 3, lemmu 18, tvrdenie 20, vetu 21, lemmy 23 a 24. Ďalej sme dokázali tvrdenie 6, pri ktorom sa všetky použité zdroje odvolávajú na pôvodný článok Gabidulin (1985), lemmu 8 a vetu 19. Obzvlášť dôležitým sa nám zdalo zrozumiteľne a zároveň podrobne popísať algoritmus opravy chýb, ktorý nevyužíva prehľadávanie okolia kódových slov hrubou silou. Dôležitosť tohto kroku spočívala predovšetkým v jeho potrebnosti pre definovanie kryptosystému. Navyše, vo väčšine citovaných zdrojoch sa efektívny dekódovací algoritmus rovno predpokladá a v článku Gabidulin (1992) je popísaný bez vysvetlenia vlastností linearizovaných polynómov, na ktorých je postavený.

Druhá kapitola práce formálne definuje asymetrický kryptosystém spolu s dvomi variantami využívajúcimi kódy hodnostnej metriky. Prvý variant, označovaný ako GPT kryptosystém, modifikuje McEliecovu schému, kedy správu transformujeme na kódove slovo a maskujeme vektorom chyby. Druhý variant modifikuje Niederreiterovu schému, kde správou je v reči samoopravných kódov priamo vektor chyby. V tejto krátkej kapitole sme poznatky z citovaného článku Overbeck a kol. (2005) doplnili predovšetkým o formálne overenie správnosti schém (lemmy 28 a 29). Zvyšok práce je zameraný práve na GPT kryptosystém, konkrétne štrukturálny útok naň vedený a možný spôsob obrany.

Analyzovaná slabina GPT kryptosystému spočíva v náročnosti skrytia štruktúry tajnej, generujúcej matice kódu vo verejnej matici zdieľanej vo verejnom kľúči. Tejto slabiny sme využili na sformulovanie Overbeckovho útoku predstaveného v kapitole 4.2 článku Overbeck a kol. (2005). Najprv sme popísali ideu tohto útoku s dokázaním lemm 31 a 32 a následne ju vlastným pričinením rozšírili o konkrétny postup, ako útok previesť na získanie alternatívneho súkromného kľúča z verejného kľúča (podkapitoly 3.1.1 a 3.1.2). Správnosť postupu sme ilustrovali na príklade prelomenia bezpečnosti GPT kryptosystému, ktorý je spolu s ostatnými príkladmi v tejto kapitole našim prínosom. Pretože tento útok má predpoklad pre svoju úspešnosť, tak sme ďalej zhrnuli známe spôsoby voľby počiatočných parametrov popísané v 5. kapitole práce Rashwan a kol. (2010), aby ho nebolo možné použiť. Treba však mať na pamäti, že tieto voľby môžu byť opäť napadnuteľné iným útokom na GPT kryptosystém.

Zoznam použitej literatúry

Barto, L. a Tůma, J. Konečná tělesa. URL https://www2.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf.

Berger, T. a Loidreau, P. (2002). Security of the Niderreiter Form of the GPT public-key cryptosystem. *Proceedings IEEE International Symposium on Information Theory, Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on, Information theory*, page 1. ISSN edseee.IEEEConferenc. doi: 10.1109/ISIT.2002.1023539.

Drápal, A. Samoopravné kódy. URL https://www2.karlin.mff.cuni.cz/~holub/soubory/drapal_kody.pdf.

Gabidulin, E. M. (1985). Theory of Codes with Maximum Rank Distance. *Problems of Information Transmission*, **21**(1), 12.

Gabidulin, E. M. (1992). A fast matrix decoding algorithm for rank-error-correcting codes. *Algebraic Coding - 1st French-Soviet Workshop, Proceedings*, **573 LNCS**, 126 – 133. ISSN 16113349. doi: 10.1007/bfb0034349.

Horlemannová-Trautmannová, A.-L., Marshall, K. a Rosenthal, J. (2017). Extension of Overbeck's attack for Gabidulin-based cryptosystems. *Designs, Codes and Cryptography: An International Journal*, page 22. ISSN 09251022. doi: 10.1007/s10623-017-0343-7.

Ourivski, A. V. a Johansson, T. (2002). New Technique for Decoding Codes in the Rank Metric and Its Cryptography Applications. *Problems of Information Transmission*, **38**(3), 237–246. ISSN 00329460. doi: 10.1023/a:1020369320078.

Overbeck, R., Dawson, E. a Vaudenay, S. (2005). A New Structural Attack for GPT and Variants. *Progress in Cryptology – Mycrypt 2005: First International Conference on Cryptology in Malaysia, Kuala Lumpur, Malaysia, September 28-30, 2005. Proceedings*, pages 50–63. ISSN 16113349. doi: 10.1007/11554868_5.

Rashwan, H., Gabidulin, E. M. a Honary, B. (2010). A Smart Approach for GPT Cryptosystem Based on Rank Codes. *2010 IEEE International Symposium on Information Theory*, page 5. doi: 10.1109/ISIT.2010.5513549. URL http://arxiv.org/abs/1006.0386.

Tan, C. H., Prabowo, T. F. a Lau, T. S. C. (2018). Rank Metric Code-based Signature. *2018 International Symposium on Information Theory and Its Applications (ISITA), Information Theory and Its Applications (ISITA), 2018 International Symposium on*, pages 70–74. ISSN edseee.IEEEConferenc. doi: 10.23919/ISITA.2018.8664280.

A. Prílohy

A.1 Kód k príkladu Overbeckovho útoku

```
In[1]:= m = alpha^5 + alpha^2 + 1
        baza = {1, alpha, alpha^2, alpha^3, alpha^4}
        Mul[a_, b_] := PolynomialMod[PolynomialMod[a * b, m], 2]
        Pow[a_, exp_] := PolynomialMod[PolynomialMod[Power[a, exp], m], 2]
        Inv[a_] := PolynomialExtendedGCD[m, a, Modulus → 2][[2, 2]]
        GausEli[A_] := (M = A; For[j = 1, j < Length[M], j = j + 1, (
            For[i = j + 1, i ≤ Length[M], i = i + 1, (
              M[[i]] = PolynomialMod[M[[i]] + Mul[Mul[Inv[M[[j, j]]], M[[i, j]]], M[[j]]], 2];
             )];
            Print[MatrixForm[M]])];
          M)

In[8]:= n = 5
        k = 2
        e = (n - k - 1) / 2

In[11]:= msg = {alpha, alpha^3 + alpha^2 + 1}
         error = {alpha + 1, 0, alpha + 1, 0, 0, alpha + 1, 0}

In[13]:= g = {alpha^4 + alpha^2, alpha^3 + 1,
            alpha^2 + alpha + 1, alpha^4 + alpha^2 + alpha, alpha^4 + alpha^3 + 1};
         gB = {{0, 1, 1, 0, 1}, {0, 0, 1, 1, 0}, {1, 0, 1, 1, 0}, {0, 1, 0, 0, 1}, {1, 0, 0, 1, 1}};
         MatrixForm[gB]
         MatrixRank[gB]

In[17]:= G = Table[Pow[g, 2^i], {i, 0, 1}];
         MatrixForm[G]
          G4 = Table[Pow[g, 2^i], {i, 0, 3}];
         MatrixForm[G4]

In[21]:= x1 = {alpha^4 + alpha^3, alpha^2};
         x2 = {alpha^3, alpha};
         X = {x1, x2};
         MatrixForm[X]

In[25]:= XG = {Join[x1, g], Join[x2, Pow[g, 2^1]]}

In[26]:= S = {{alpha, alpha^2 + 1}, {1, alpha^3 + alpha^2}};
         MatrixForm[S]
         GausEli[S];

In[29]:= T = {{0, 0, 1, 0, 1, 1, 0}, {1, 1, 0, 0, 0, 1, 0}, {1, 0, 1, 0, 1, 0, 1},
            {0, 1, 0, 1, 1, 1, 0}, {0, 1, 1, 0, 0, 1, 0}, {0, 0, 0, 0, 0, 1, 1}, {0, 0, 0, 1, 0, 1, 1}};
         MatrixForm[T]
         MatrixRank[T]

In[33]:= GV = PolynomialMod[PolynomialMod[S.XG.T, m], 2];
         MatrixForm[GV]

In[35]:= ciph = PolynomialMod[PolynomialMod[msg.GV + error, m], 2]

In[36]:= GRV = Table[Pow[GV[[j]], 2^i], {i, 0, 2}, {j, 1, 2}];
         GRV = Join[GRV[[1]], GRV[[2]], GRV[[3]]];
         MatrixForm[GRV]

In[39]:= GGRV = GRV;
        For[j = 1, j ≤ 6, j = j + 1, (
          GGRV[[j]] = Mul[Inv[GGRV[[j, j]]], GGRV[[j]]];
          For[i = j + 1, i ≤ Length[GGRV], i = i + 1, (
            GGRV[[i]] = PolynomialMod[GGRV[[i]] + Mul[GGRV[[i, j]], GGRV[[j]]], 2];
           )];
          Print[MatrixForm[GGRV]])]
```

```
In[41]:= u7 = a;
         u6 = (1 + alpha^2 + alpha^3 + alpha^4) u7;
         u5 = Mul[(1 + alpha^3), u6];
         u4 = Mul[1, alpha * u5 + (alpha^2 + alpha^3) u6 + (1 + alpha) u7];
         u3 = Mul[1,
             (1 + alpha^2) u4 + (1 + alpha^3 + alpha^4) u5 + (alpha^4) u6 + (1 + alpha + alpha^3 + alpha^4) * u7];
         u2 = Mul[1,  (1 + alpha + alpha^2 + alpha^3 + alpha^4) u3 + (alpha^2 + alpha^4) u4 +
              (alpha^2 + alpha^3 + alpha^4) u5 + (alpha^2 + alpha^4) u6 + (alpha + alpha^3) u7];
         u1 = Mul[1, (alpha + alpha^2 + alpha^4) u2 + (alpha + alpha^4) u3 + (1 + alpha + alpha^3) * u4 +
              (alpha^2 + alpha^3) u5 + (1 + alpha + alpha^3 + alpha^4) u6 + (1 + alpha + alpha^3) u7];
         u = {u1, u2, u3, u4, u5, u6, u7}

In[49]:= PolynomialMod[PolynomialMod[GRV.u, m], 2]

In[50]:= u = PolynomialMod[PolynomialMod[u /. {a → alpha}, m], 2];
         MatrixForm[u]

In[52]:= uBaza = {{1, 0, 1, 1, 0, 1, 0}, {0, 1, 1, 1, 0, 1, 1},
            {1, 0, 0, 0, 1, 1, 0}, {0, 1, 0, 1, 1, 1, 0}, {0, 1, 0, 0, 1, 1, 0}};
         hBaza = Transpose@{uBaza[[ ;; , 2]], uBaza[[ ;; , 3]],
            uBaza[[ ;; , 4]], uBaza[[ ;; , 5]], uBaza[[ ;; , 7]]}
         MatrixForm[uBaza]
         MatrixRank[uBaza]
         MatrixForm[hBaza]
         MatrixRank[hBaza]

In[58]:= hF = {u[[2]], u[[3]], u[[4]], u[[5]], u[[7]]};
         MatrixForm[hF]

In[60]:= Tvlnka = {{1, 1, 0, 1, 0}, {0, 1, 0, 1, 0}}
         MatrixForm[PolynomialMod[Tvlnka.Transpose[hBaza], 2]]

In[62]:= TFInv = Mod[{{1, 0, 0, 0, 0, 0, 0}, {0, 0, 1, 0, 0, 0, 0}, {0, 0, 0, 1, 0, 0, 0},
               {0, 0, 0, 0, 1, 0, 0}, {0, 0, 0, 0, 0, 1, 0}, {0, 1, 0, 0, 0, 0, 0}, {0, 0, 0, 0, 0, 0, 1}}.
              {{1, 0, 1, 1, 0, 1, 0}, {0, 1, 0, 1, 0, 1, 0}, {0, 0, 1, 0, 0, 0, 0}, {0, 0, 0, 1, 0, 0, 0},
               {0, 0, 0, 0, 1, 0, 0}, {0, 0, 0, 0, 0, 1, 0}, {0, 0, 0, 0, 0, 0, 1}}, 2];
         MatrixForm[
          TFInv]

In[64]:= PolynomialMod[Join[{0, 0}, hF].Transpose[TFInv], 2] == u

In[65]:= HF = Table[Pow[hF, 2^(5 - (2 - i))], {i, 0, 2}]

In[66]:= GF = PolynomialMod[PolynomialMod[(GV.TFInv)[[ ;; , 3 ;; 7]], m], 2];
         MatrixForm[GF]

In[68]:= PolynomialMod[PolynomialMod[GF.Transpose[HF], m], 2]

In[69]:= y = PolynomialMod[(ciph - error).TFInv, 2][[3 ;;]]

In[70]:= x = {x11, x22}

In[71]:= sust = Transpose[Join[GF, {y}]];
         MatrixForm[sust]

In[73]:= For[j = 1, j ≤ 2, j = j + 1, (
           sust[[j]] = Mul[Inv[sust[[j, j]]], sust[[j]]];
           For[i = j + 1, i ≤ Length[sust], i = i + 1, (
             sust[[i]] =  PolynomialMod[sust[[i]] + Mul[sust[[i, j]], sust[[j]]], 2];
            )];
           Print[MatrixForm[sust]])]

In[74]:= x22 = 1 + alpha^2 + alpha^3;
         x11 = PolynomialMod[Mul[alpha + alpha^2, x22] + 1 + alpha^3, 2];
         x

In[77]:= x == msg
```