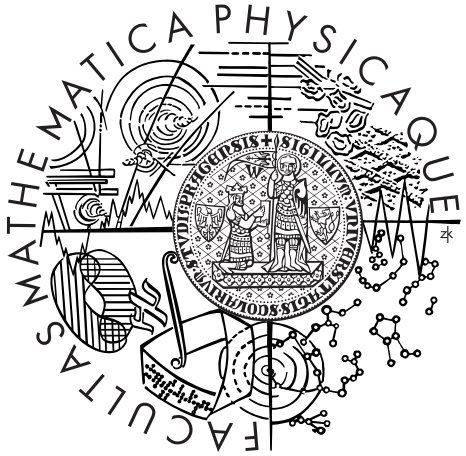
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Tereza Hrubešová

Klasický strukturální útok na Niederreiterův kryptosystém vytvořený nad GRS kódy

Katedra algebry

Vedoucí bakalářské práce:	prof. RNDr. Aleš Drápal, CSc., DSc.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti

Praha 2014

Děkuji prof. RNDr. Alešovi Drápalovi, CSc., DSc. za ochotu a trpělivost, se kterými vedl mou bakalářskou práci, za vstřícnost při konzultacích i poskytnutí potřebné literatury.

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

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

V ..... dne ..... Tereza Hrubešová

Název práce: Klasický strukturální útok na Niederreiterův kryptosystém vytvořený nad GRS kódy

Autor: Tereza Hrubešová

Katedra: Katedra algebry

Vedoucí bakalářské práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Hlavním cílem této bakalářské práce je popis útoku na Niederreiterův kryptosystém vytvořený nad GRS kódy. Tento útok byl zveřejněn v roce 1992 Sidelnikovem a Šestakovem. Na začátku práce je uvedena problematika působení grupy na množině, která je použita v samotném útoku. Následuje stručný úvod do teorie samoopravných kódů, jsou popsány GRS kódy a představeny McEliecův a Niederreiterův kryptosystém, oba jako zástupci post-kvantové kryptografie. Další část práce je věnována samotnému útoku. Je ukázáno, jakým způsobem využijeme působení grupy na množině, dále je podrobně popsán průběh útoku a zmíněna jeho časová složitost. Vše je také ilustrováno na příkladech.

Klíčová slova: Zobecněné Reed-Solomonovy kódy, Post-kvantová kryptografie, McEliecův kryptosystém, Niederreiterův kryptosystém

Title: Classical structural attack on the Niederreiter cryptosystem based upon GRS codes

Author: Tereza Hrubešová

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: The main purpose of this bachelor thesis is the description of the attack on the Niederreiter cryptosystem based on GRS codes. This attack was published by Sidelnikov and Shestakov in 1992. In the beginning the problem of group action, which is used in the attack, is introduced. A short preface into the coding theory follows, GRS codes are described and McEliece and Niederreiter cryptosystems are introduced, both as representatives of post-quantum cryptography. The following part of the thesis is dedicated to the attack itself. It is showed how one uses the group action, the process of the attack is also described in detail and its computing complexity is mentioned. Everything is illustrated by examples.

Keywords: Generalized Reed-Solomon codes, Post-quantum cryptography, McEliece cryptosystem, Niederreiter cryptosystem

Obsah

Úvod

V dnešní době, kdy je značná pozornost věnována výzkumu v oblasti kvantových počítačů, dochází přirozeně také k rozvoji post-kvantové kryptografie. Ta se zabývá kryptosystémy s veřejným klíčem, proti kterým nejsou známy žádné efektivní útoky pomocí kvantových počítačů. V současnosti se v praxi používají asymetrické šifry založené nejčastěji na problému faktorizace či diskrétního logaritmu. Tyto šifry by ovšem proti síle výkonných kvantových počítačů neobstály. Bylo by je totiž možné zlomit v polynomiálním čase pomocí Shorova algoritmu.

Post-kvantová kryptografie je dnes rozvíjena ve třech hlavních směrech: jednak je to kryptografie založená na mřížích, dále takzvaná algebraická kryptografie, která se opírá v současných modelech především o složitost konjugace v nekomutativních grupách, a konečně kryptografie využívající samoopravné kódy. Zástupcem posledně zmíněné oblasti je McEliecův kryptosystém a jeho mladší obdoba - kryptosystém Niederreiterův. McEliecův kryptosystém využívá ve své původní podobě Goppa kódy a proti tomuto návrhu zatím není znám žádný efektivní útok. Existují ale i další návrhy, lišící se především typem používaných kódů. Proti některým jsou známy efektivní útoky, proti jiným se stále hledají. I z tohoto důvodu je dobré znát útoky již popsané. Na základě jejich znalosti se můžeme poučit z chyb, vyvarovat se jich při návrzích nových kryptosystémů, případně pomocí nich objevit slabiny stávajících návrhů.

Jedním z těchto známých útoků se zabývá i tato práce. Konkrétně se jedná o útok na Niederreiterův kryptosystém vytvořený nad GRS kódy.

V práci je stručně uvedena problematika samoopravných kódů, jsou zde definovány GRS kódy, dokázány některé jejich vlastnosti a nastíněno jejich dekódování. Následně je představen McEliecův a Niederreiterův kryptosystém. Poté je popsán samotný útok, který v roce 1992 zveřejnili Sidelnikov a Šestakov [1]. Tento útok využívá teorii působení grupy na množině (konkrétně grupy lineárních lomených transformací), která je obsahem první kapitoly práce. Vše je také ilustrováno na jednoduchých příkladech.

Kapitola 1

Lineární lomené transformace

1.1 Působení grupy na množině

Definice 1.1. *Projektivní přímka nad tělesem F je jednodimenzionální projektivní prostor, tedy množina všech jednodimenzionálních podprostorů (tj. přímek procházejících počátkem) v dvoudimenzionálním vektorovém prostoru $V = F \times F$.*

Projektivní přímku nad tělesem F budeme značit $\mathbb{P}^1(F)$.

Projektivním bodem pak rozumíme každý jednodimenzionální podprostor V, tj. každou přímku procházející počátkem. Obsahuje-li tato přímka nenulový bod $(x_1, x_2)^\top \in V$, značíme příslušný projektivní bod $[x_1 : x_2]$ (zápis pomocí homogenních souřadnic). Pro každé $\lambda \in F^*$ zjevně platí $[x_1 : x_2] = [\lambda x_1 : \lambda x_2]$. Pro $x_2 \neq 0$ je $[x_1 : x_2] = [\frac{x_1}{x_2} : 1]$. Každý projektivní bod projektivní přímky je tedy možné jednoznačně zapsat jako $[x : 1], x \in F$, nebo jako $[1 : 0]$. Z toho vyplývá, že projektivní přímku můžeme ztotožnit s množinou $F \cup \{\infty\}$, kde $x \in F$ značí projektivní bod $[x : 1]$ a ∞ značí projektivní bod $[1 : 0]$. Množinu $F \cup \{\infty\}$ budeme dále značit F_∞.

Na F_∞ částečně dodefinujeme aritmetiku následujícím způsobem:

$$\frac{x}{0} = \infty, \quad \frac{x}{\infty} = 0, \quad x \cdot \infty = \infty, \quad \text{pokud } x \in F^*;$$

$$x + \infty = \infty, \quad \text{pokud } x \in F.$$

Definice 1.2. *Nechť $\boldsymbol{G}$ je grupa a X neprázdná množina. Zobrazení $* : \boldsymbol{G} \times X \to X$ nazveme působením grupy $\boldsymbol{G}$ na množině X, pokud:*

1. *$h * (g * x) = (hg) * x$ pro všechna $g, h \in \boldsymbol{G}, x \in X$; a*
2. *$e * x = x$ pro všechna $x \in X$ (e je jednotkový prvek grupy $\boldsymbol{G}$).*

Nechť $\boldsymbol{G}$ působí na X. Když pro pevně zvolené $g \in \boldsymbol{G}$ označíme π_g zobrazení $\pi_g : X \to X$ dané předpisem $x \mapsto g * x$, bude podle ([2]; Věta 1.1.4) platit:

- pro libovolné $g \in \boldsymbol{G}$ je π_g permutace na množině X; a
- zobrazení $\pi : \boldsymbol{G} \to \boldsymbol{S}(X)$ dané vztahem $g \mapsto \pi_g$ je homomorfismus grup ($\boldsymbol{S}(X)$ je grupa všech permutací na množině X).

Definice 1.3. *Permutační grupa na množině X je podgrupa $\boldsymbol{S}(X)$.*

Nechť $\boldsymbol{GL}(2,F)$ je grupa invertibilních matic typu 2×2 nad tělesem F. Jednotkovou matici řádu dva budeme značit jako $\boldsymbol{I}_2$. Dále nechť $\boldsymbol{M}$, $\boldsymbol{N}$ jsou libovolné prvky $\boldsymbol{GL}(2,F)$ a W projektivní bod, tj. $W=\langle(x,1)^\top\rangle$, kde $x\in F$, nebo $W=\langle(1,0)^\top\rangle$. Působení grupy $\boldsymbol{GL}(2,F)$ na projektivní přímce $\mathbb{P}^1(F)$ je dané vztahem:

$$\boldsymbol{M}*W=\boldsymbol{M}W=\{\boldsymbol{M}w; w\in W\}.$$

Protože

$$(\boldsymbol{MN})*W=(\boldsymbol{MN})W=\boldsymbol{M}(\boldsymbol{N}W)=\boldsymbol{M}(\boldsymbol{N}*W)=\boldsymbol{M}*(\boldsymbol{N}*W)$$

a

$$\boldsymbol{I}_2*W=\boldsymbol{I}_2W=W,$$

jedná se skutečně o působení grupy na množině.

Je-li $W=\langle(x,1)^\top\rangle$ a $\boldsymbol{M}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ libovolný prvek $\boldsymbol{GL}(2,F)$, tak $\boldsymbol{M}*W$ obsahuje bod $(ax+b,cx+d)^\top$. Proto $\boldsymbol{M}*W$ ztotožňujeme v tomto případě s $(ax+b)/(cx+d)$. Používáme přitom dříve dodefinovanou aritmetiku. To znamená, že pokud $cx+d=0$, tento zlomek dává ∞. Podobně pokud $W=\langle(1,0)^\top\rangle$, $\boldsymbol{M}*W$ obsahuje bod (a,c) a $\boldsymbol{M}*W$ pak ztotožňujeme s a/c. Pokud $c=0$, zlomek dává ∞. Můžeme tedy popsat ekvivalentní působení grupy $\boldsymbol{GL}(2,F)$ na množině F_∞ následovně:

$$\boldsymbol{M}*x=\begin{pmatrix}a & b\\ c & d\end{pmatrix}*x=\begin{cases}\frac{ax+b}{cx+d}, & \text{pokud } x\in F\\ \frac{a}{c}, & \text{pokud } x=\infty.\end{cases}$$

Zobrazení $\pi:\boldsymbol{GL}(2,F)\to\boldsymbol{S}(F_\infty)$ je homomorfismus grup. Proto $\mathbf{Im}\ \pi\leq\boldsymbol{S}(F_\infty)$ je permutační grupa na F_∞. Jsou to právě všechna zobrazení tvaru $x\mapsto(ax+b)/(cx+d)$, kde a, b, c, $d\in F$ a $ad-bc\neq 0$. Tato zobrazení se nazývají *lineární lomené transformace*. Grupu $\mathbf{Im}\ \pi$ budeme značit $\boldsymbol{PGL}(2,F)$ a nazývat *projektivní lineární grupa* nebo také *grupa lineárních lomených transformací*.

Lemma 1.1. *Nechť* $\boldsymbol{M}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\boldsymbol{GL}(2,F)$. *Pak*

$$\pi_{\boldsymbol{M}}(\infty)=\frac{a}{c},\quad \pi_{\boldsymbol{M}}(0)=\frac{b}{d},\quad \pi_{\boldsymbol{M}}(1)=\frac{a+b}{c+d}.$$

Důkaz. Stačí dosadit do předpisu pro působení grupy. ❑

Důsledek 1.2.

$$\boldsymbol{M}\in\operatorname{Ker}\pi\ \leftrightarrow\ \boldsymbol{M}=\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\ \textit{pro nějaké}\ \lambda\in F^*.$$

Důkaz. Platí $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{Ker} \pi \leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} * x = x$ pro všechna $x \in F_\infty$.

Po dosazení $x = \infty$ dostáváme $a/c = \infty$, z čehož plyne $c = 0$. Pro $x = 0$ máme $b/d = 0$, a tedy $b = 0$. A nakonec po dosazení $x = 1$ dostaneme $a = d$. Navíc musí platit $a, d \in F^*$.

Naopak je-li $\lambda \in F^*$ a $\boldsymbol{M} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, pak $\boldsymbol{M} * x = \lambda x/\lambda = x$ pro všechna $x \in F$ a $\boldsymbol{M} * \infty = \lambda/0 = \infty$.

❑

Důsledek 1.3.

$$\boldsymbol{GL}(2, F)/(F^* \boldsymbol{I}_2) \cong \boldsymbol{PGL}(2, F).$$

Důkaz. Plyne z první věty o izomorfismu.

❑

1.2 3-tranzitivita permutační grupy

Definice 1.4. *Permutační grupa $\boldsymbol{G}$ na X je tranzitivní, pokud*

$$\forall a, b \in X : \exists \phi \in \boldsymbol{G} : \phi(a) = b.$$

Lemma 1.4. *Permutační grupa $\boldsymbol{PGL}(2, F)$ na F_∞ je tranzitivní.*

Důkaz. Stačí ukázat, že pro libovolný pevně zvolený bod $\beta \in F_\infty$ a pro všechny body $\alpha \in F_\infty$ existuje $\phi_\alpha \in \boldsymbol{PGL}(2, F)$ tak, že $\phi_\alpha(\beta) = \alpha$. Námi požadované zobrazení, které zobrazí a na b, pak bude $\phi_b \phi_a^{-1}$. Za β zvolíme ∞. Pro $\alpha \in F$ definujeme ϕ_α jako $(\alpha x + 1)/x = \alpha + 1/x$ a ϕ_∞ definujeme jako id_{F_∞}.

❑

Definice 1.5. *Permutační grupa $\boldsymbol{G}$ na X se nazývá 3-tranzitivní, pokud pro každé dvě trojice (a_1, a_2, a_3), $(b_1, b_2, b_3) \in X^3$ takové, že $a_i \neq a_j$ a $b_i \neq b_j$, pokud $1 \leq i < j \leq 3$, existuje $\phi \in \boldsymbol{G}$, jež splňuje $\phi(a_i) = b_i$, $1 \leq i \leq 3$. Pokud takové zobrazení existuje vždy právě jedno, grupa se nazývá ostře 3-tranzitivní.*

Tvrzení 1.5. *Permutační grupa $\boldsymbol{PGL}(2, F)$ na F_∞ je ostře 3-tranzitivní.*

Důkaz. Z podobného důvodu jako v důkazu lemmatu 1.4 stačí ukázat, že existuje právě jedno $\phi \in \boldsymbol{PGL}(2, F)$ takové, že $\phi(\infty) = \alpha$, $\phi(0) = \beta$ a $\phi(1) = \gamma$ pro libovolnou trojici po dvou různých $\alpha, \beta, \gamma \in F_\infty$.

Existence:

Ukážeme, že stačí najít $\mu_\alpha, \nu_{\beta'}, \psi_{\gamma'} \in \boldsymbol{PGL}(2, F)$, kde

- $\mu_\alpha(\infty) = \alpha, \quad \alpha \in F_\infty$;
- $\nu_{\beta'}(\infty) = \infty, \quad \nu_{\beta'}(0) = \beta', \quad \beta' \in F$;

- $\psi_{\gamma'}(\infty) = \infty, \quad \psi_{\gamma'}(0) = 0, \quad \psi_{\gamma'}(1) = \gamma', \quad \gamma' \in F^*$.

Předpokládejme, že máme prvky $\boldsymbol{PGL}(2, F)$ s těmito vlastnostmi. Uvažme nyní $\phi = \mu_\alpha \nu_{\beta'} \psi_{\gamma'}$. Pak

- $\phi(\infty) = (\mu_\alpha \nu_{\beta'} \psi_{\gamma'})(\infty) = (\mu_\alpha \nu_{\beta'})(\psi_{\gamma'}(\infty)) = (\mu_\alpha \nu_{\beta'})(\infty) = \mu_\alpha(\nu_{\beta'}(\infty)) = = \mu_\alpha(\infty) = \alpha$;
- $\phi(0) = (\mu_\alpha \nu_{\beta'} \psi_{\gamma'})(0) = (\mu_\alpha \nu_{\beta'})(\psi_{\gamma'}(0)) = (\mu_\alpha \nu_{\beta'})(0) = \mu_\alpha(\nu_{\beta'}(0)) = \mu_\alpha(\beta')$;
- $\phi(1) = (\mu_\alpha \nu_{\beta'} \psi_{\gamma'})(1) = (\mu_\alpha \nu_{\beta'})(\psi_{\gamma'}(1)) = (\mu_\alpha \nu_{\beta'})(\gamma') = \mu_\alpha(\nu_{\beta'}(\gamma'))$.

Pokud položíme $\beta' = \mu_\alpha^{-1}(\beta)$, pak $\phi(0) = \mu_\alpha(\mu_\alpha^{-1}(\beta)) = (\mu_\alpha \mu_\alpha^{-1})(\beta) = \beta$. Stejně pokud položíme $\gamma' = (\nu_{\beta'}^{-1} \mu_\alpha^{-1})(\gamma)$, dostáváme $\phi(1) = \gamma$. Vidíme, že ϕ je námi hledaný prvek grupy $\boldsymbol{PGL}(2, F)$.

Zbývá nalézt μ_α, $\nu_{\beta'}$ a $\psi_{\gamma'} \in \boldsymbol{PGL}(2, F)$. Dané požadavky splňují následující transformace:

$$\mu_\alpha(x) = \begin{cases} \frac{\alpha x + 1}{x}, & \alpha \in F \\ x, & \alpha = \infty \end{cases} ; \quad \nu_{\beta'}(x) = x + \beta'; \quad \psi_{\gamma'}(x) = \gamma' x.$$

Jednoznačnost:

Budiž $\phi, \rho \in \boldsymbol{PGL}(2, F)$ splňující $\phi(\infty) = \rho(\infty) = \alpha$, $\phi(0) = \rho(0) = \beta$ a $\phi(1) = \rho(1) = \gamma$. Pak platí: $\rho^{-1}\phi(\infty) = \infty$, $\rho^{-1}\phi(0) = 0$ a $\rho^{-1}\phi(1) = 1$. Nechť $\rho^{-1}\phi = (ax + b)/(cx + d)$, kde $a, b, c, d \in F$ a $ad - bc \neq 0$. Z $\rho^{-1}\phi(\infty) = \infty$ plyne $c = 0$, z $\rho^{-1}\phi(0) = 0$ plyne $b = 0$ a z $\rho^{-1}\phi(1) = 1$ plyne $a/d = 1$. Vidíme, že $\rho^{-1}\phi(x) = x$, a tedy $\phi = \rho$.

❑

Lemma 1.6.

$$\boldsymbol{PGL}(2, F) = \langle 1/x, ax + b; a \in F^*, b \in F \rangle.$$

Důkaz. Označme $\boldsymbol{H} = \langle 1/x, ax + b; a \in F^*, b \in F \rangle$. Pak $\boldsymbol{H} \leq \boldsymbol{PGL}(2, F)$. Definujeme μ_α, $\nu_{\beta'}$, $\psi_{\gamma'}$ jako v důkazu tvrzení 1.5. Víme, že každý prvek $\phi \in \boldsymbol{PGL}(2, F)$ lze zapsat jako $\mu_\alpha \nu_{\beta'} \psi_{\gamma'}$. Protože $\nu_{\beta'} \in \boldsymbol{H}$ a $\psi_{\gamma'} \in \boldsymbol{H}$, stačí ukázat, že $\mu_\alpha \in \boldsymbol{H}$. Platí $\mu_\alpha(x) = (\alpha x + 1)/x = (x + \alpha) \circ (1/x) \in \boldsymbol{H}$.

❑

Kapitola 2

Samoopravné kódy

2.1 Úvod do teorie kódů

Definice 2.1. *Nechť $\mathbb{A}$ je konečná abeceda, tj. množina symbolů o velikosti q. Potom $[n,k]_q$ (blokovým) kódem $\mathcal{C}$ nad $\mathbb{A}$ rozumíme neprázdnou podmnožinu $\mathbb{A}^n$ takovou, že $k = \log_q |\mathcal{C}|$.*

Prvky $\mathbb{A}^n$ nazýváme *slova*, prvky $\mathcal{C}$ *kódová slova*. Slovo značíme $u = (u_1, \ldots, u_n)$, kde $u_i \in \mathbb{A}$.

Definice 2.2. *Hammingovu vzdálenost slov u,$v \in \mathbb{A}^n$ definujeme jako*

$$d(u,v) = |\{i \in \{1,\ldots,n\};\ u_i \neq v_i\}|.$$

Definice 2.3. *Minimální vzdálenost kódu $\mathcal{C}$ definujeme jako*

$$d(\mathcal{C}) = \min\{d(u,v);\ u,v \in \mathcal{C}, u \neq v\},\ \textit{pokud}\ |\mathcal{C}| > 1,$$

$$d(\mathcal{C}) := n+1,\ \textit{pokud}\ |\mathcal{C}| = 1.$$

Značení: $[n,k,d]_q$ kód je každý $[n,k]_q$ kód s minimální vzdáleností d.

Definice 2.4. *Nechť F je konečné těleso a $u \in F^n$. Hammingovu váhu slova u definujeme jako*

$$w(u) = |\{i \in \{1,\ldots,n\};\ u_i \neq 0\}| = d(u,0).$$

Definice 2.5. *Nechť F je konečné těleso. Pak $[n,k,d]_q$ kód $\mathcal{C}$ nazýváme lineární, pokud $\mathcal{C}$ je podprostor vektorového prostoru F^n.*

Lemma 2.1. *Buď $\mathcal{C}$ lineární $[n,k,d]_q$ kód. Pak*

$$d = \min\{w(u);\ u \in \mathcal{C} \setminus \{0\}\}.$$

Důkaz. Protože $\mathcal{C}$ je lineární, bude platit

$$u_1,\ u_2 \in \mathcal{C} \to u_1 - u_2 \in \mathcal{C}.$$

Dále $d(u_1, u_2) = w(u_1 - u_2)$ a odtud plyne:

$$d = \min\{d(u_1, u_2);\ u_1, u_2 \in \mathcal{C}, u_1 \neq u_2\} =$$

$$= \min\{w(u_1 - u_2);\ u_1, u_2 \in \mathcal{C}, u_1 \neq u_2\} = \min\{w(u);\ u \in \mathcal{C} \setminus \{0\}\}.$$

❑

Definice 2.6. *Buď $\mathcal{C}$ lineární $[n, k, d]_q$ kód. Matici $\boldsymbol{C}$ typu $k \times n$ nazveme generující maticí kódu $\mathcal{C}$, obsahuje-li v řádcích právě bázi podprostoru $\mathcal{C}$. Prověrková matice $\boldsymbol{H}$ kódu $\mathcal{C}$ je matice $(n-k) \times n$, pro kterou platí: $u \in \mathcal{C} \leftrightarrow \boldsymbol{H}u^\top = 0$.*

Buď $\mathcal{C}$ lineární $[n, k, d]_q$ kód nad F a $\boldsymbol{C}$ jeho generující matice. Pak pro kódování slova $u \in F^k$ budeme používat zobrazení $F^k \to \mathcal{C}$ dané vztahem $u \mapsto u\boldsymbol{C}$.

Při přenosu kódového slova $c \in F^n$ může dojít k chybě a obdržené slovo $v \in F^n$ bude tvaru $v = c + e$, kde $e \in F^n$ nazýváme *chybové slovo*. Kód s minimální vzdáleností d může opravit maximálně $t = \lfloor \frac{d-1}{2} \rfloor$ chyb ([3]; Tvrzení 1.3). Budeme tedy předpokládat, že $w(e) \leq \lfloor \frac{d-1}{2} \rfloor$. Problém dekódování $v \in F^n$ na nejbližší kódové slovo spočívá v nalezení kódového slova $c \in \mathcal{C}$, které minimalizuje hodnotu $d(v, c)$, nebo ekvivalentně v nalezení slova $e \in F^n$ minimální Hammingovy váhy takového, že $v - e \in \mathcal{C}$.

Definice 2.7. *Buď $\mathcal{C}$ lineární $[n, k, d]_q$ kód nad F a $u \in F^n$. Rozkladovou třídou kódu $\mathcal{C}$ obsahující u nazýváme množinu $u + \mathcal{C} = \{u + c; c \in \mathcal{C}\}$.*

Definice 2.8. *Nechť $\mathcal{C}$ je lineární $[n, k, d]_q$ kód nad tělesem F a $\boldsymbol{H}$ jeho prověrková matice. Pak syndrom slova $u \in F^n$ definujeme jako*

$$s = \boldsymbol{H}u^\top.$$

Kódová slova jsou právě slova, jejichž syndrom je nulový. Pro dvě slova u_1, u_2 platí

$$u_1 - u_2 \in \mathcal{C} \leftrightarrow \boldsymbol{H}u_1^\top = \boldsymbol{H}u_2^\top.$$

To znamená, že dvě slova u_1, u_2 jsou ve stejné rozkladové třídě kódu $\mathcal{C}$ právě tehdy, když se jejich syndromy rovnají.

Dekódování na nejbližší slovo pomocí syndromu se pak skládá z nalezení syndromu obdrženého slova u (spočítání $s = \boldsymbol{H}u^\top$) a nalezení slova $e \in F^n$ ze stejné rozkladové třídy s minimální Hammingovou váhou v rámci této třídy (tj. slova $e \in F^n$ minimální Hammingovy váhy, pro které platí $s = \boldsymbol{H}e^\top$). Při spočítání syndromu jde o vynásobení vektoru maticí. Nalezení slova e je ale v případě obecného lineárního kódu složité (jedná se o NP-úplný problém). Pro některé kódy se speciální strukturou ovšem existují efektivní dekódovací algoritmy. Více o dekódování některých lineárních kódů lze nalézt v [3].

Definice 2.9. *Buď $\mathcal{C}$ lineární $[n, k, d]_q$ kód. Řekneme, že jeho generující matice $\boldsymbol{C}$ je ve standardním tvaru, pokud $\boldsymbol{C} = (\boldsymbol{I}_k \mid \boldsymbol{A})$, kde $\boldsymbol{I}_k$ je jednotková matice $k \times k$ a $\boldsymbol{A}$ matice typu $k \times (n-k)$.*

Tvrzení 2.2. *Buď $\boldsymbol{H}$ prověrková matice lineárního kódu $\mathcal{C} \neq \{0\}$. Minimální vzdálenost kódu $\mathcal{C}$ je největší d takové, že každá množina $d-1$ sloupců v $\boldsymbol{H}$ je lineárně nezávislá.*

Důkaz. Buď $\boldsymbol{H} = (h_1\ h_2\ \ldots\ h_n)$ prověrková matice lineárního kódu $\mathcal{C} \neq \{0\}$, $u = (u_1, \ldots, u_n)$ kódové slovo kódu $\mathcal{C}$ s nenulovou Hammingovou váhou a $i_1, \ldots, i_k$ nechť jsou právě všechny nenulové pozice u. Vztah $\boldsymbol{H}u^\top = 0$ pak vyjadřuje lineární závislost sloupců $h_{i_1}, \ldots, h_{i_k}$ matice $\boldsymbol{H}$. Minimální vzdálenost kódu je d, tedy z tvrzení 2.1 víme, že tento kód obsahuje slovo o Hammingově váze právě d, ale neobsahuje žádné slovo o menší Hammingově váze. Proto každá množina $d-1$ sloupců v $\boldsymbol{H}$ je lineárně nezávislá, ale najdeme d sloupců, které jsou lineárně závislé.

❑

Tvrzení 2.3 (Singletonův odhad)**.** *Pro každý lineární $[n, k, d]_q$ kód je*

$$d \leq n - k + 1.$$

Důkaz. Prověrková matice $\boldsymbol{H}$ obsahuje regulární matici s hodností nejvýše $n-k$ (počet řádků $\boldsymbol{H}$). Podle tvrzení 2.2 potom platí $d - 1 \leq n - k$.

❑

Definice 2.10. *Řekneme, že $[n, k, d]_q$ kód je MDS (maximum distance separable) kód, jestliže $d = n - k + 1$.*

Definice 2.11. *Buď $\mathcal{C}$ lineární $[n, k]_q$ kód nad F. Duálním kódem kódu $\mathcal{C}$ nazveme kód*

$$\mathcal{C}^\perp = \{x \in F^n; \boldsymbol{C}x^\top = 0\},$$

kde $\boldsymbol{C}$ je generující matice kódu $\mathcal{C}$.

Poznámka. Duální kód $\mathcal{C}^\perp$ je lineární $[n, n-k]_q$ kód nad F, jehož prověrkovou maticí je matice $\boldsymbol{C}$. Naopak generující maticí kódu $\mathcal{C}^\perp$ je prověrková matice kódu $\mathcal{C}$.

2.2 Zobecněné Reed-Solomonovy kódy

Definice 2.12. *Nechť $\mathbb{F}_q$ je konečné těleso, dále $\alpha_1, \alpha_2, \ldots, \alpha_n$ po dvou různé nenulové prvky $\mathbb{F}_q$ a $v_1, v_2, \ldots, v_n$ nenulové prvky $\mathbb{F}_q$. Zobecněný Reed-Solomonův (GRS) kód nad $\mathbb{F}_q$ je lineární $[n, k, d]_q$ kód nad $\mathbb{F}_q$ s prověrkovou maticí*

$$\boldsymbol{H}_{GRS} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \ldots & \alpha_n^{n-k-1} \end{pmatrix} \begin{pmatrix} v_1 & 0 & \ldots & 0 \\ 0 & v_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & v_n \end{pmatrix}.$$

Definice 2.12 je obvykle uváděnou definicí GRS kódu. Pro potřeby útoku, který bude ukázán později, uvedeme ještě rozšířenou definici GRS kódu. Budeme v ní uvažovat dodefinovanou aritmetiku z první kapitoly. Dále ještě definujme 0^0 jako 1.

Definice 2.13. *Buď $F = \mathbb{F}_q$ konečné těleso a $F_\infty = \mathbb{F}_q \cup \infty$. Dále $\alpha_1, \alpha_2, \ldots, \alpha_n$ nechť jsou po dvou různé prvky F_∞ a $v_1, v_2, \ldots, v_n$ nenulové prvky F. Zobecněný Reed-Solomonův (GRS) kód je lineární $[n, k, d]_q$ kód s prověrkovou maticí*

$$\boldsymbol{H}_{GRS} = \begin{pmatrix} v_1\alpha_1^0 & v_2\alpha_2^0 & \ldots & v_n\alpha_n^0 \\ v_1\alpha_1^1 & v_2\alpha_2^1 & \ldots & v_n\alpha_n^1 \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \ldots & v_n\alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1\alpha_1^{n-k-1} & v_2\alpha_2^{n-k-1} & \ldots & v_n\alpha_n^{n-k-1} \end{pmatrix},$$

kde pro $\alpha_i = \infty$ je i-tý sloupec tvaru $v_i(0, \ldots, 0, 1)^\top$.

Dále budeme GRS kódem rozumět kód podle definice 2.13.

Prověrkovou matici GRS kódu nazveme *kanonickou*, pokud má tvar uvedený v definici. Prvky $\alpha_1, \alpha_2, \ldots, \alpha_n$ se nazývají lokátory, prvky $v_1, v_2, \ldots, v_n$ multiplikátory. Stejný GRS kód může být definován pomocí více skupin lokátorů. Tedy ani kanonická prověrková matice kódu není unikátní.

Tvrzení 2.4. *Každý $[n,k,d]_q$ GRS kód je MDS kód, tedy $d = n - k + 1$.*

Důkaz. Podle tvrzení 2.2 stačí ukázat, že každá množina $n-k$ sloupců prověrkové matice GRS kódu je lineárně nezávislá.
Nechť σ je libovolná permutace na $1, \ldots, n$. Pak chceme dokázat, že matice tvaru

$$\begin{pmatrix} \alpha_{\sigma(1)}^0 & \alpha_{\sigma(2)}^0 & \ldots & \alpha_{\sigma(n-k)}^0 \\ \alpha_{\sigma(1)}^1 & \alpha_{\sigma(2)}^1 & \ldots & \alpha_{\sigma(n-k)}^1 \\ \alpha_{\sigma(1)}^2 & \alpha_{\sigma(2)}^2 & \ldots & \alpha_{\sigma(n-k)}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{\sigma(1)}^{n-k-1} & \alpha_{\sigma(2)}^{n-k-1} & \ldots & \alpha_{\sigma(n-k)}^{n-k-1} \end{pmatrix} \begin{pmatrix} v_{\sigma(1)} & 0 & \ldots & 0 \\ 0 & v_{\sigma(2)} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & v_{\sigma(n-k)} \end{pmatrix}$$

je regulární.

Pokud $\alpha_{\sigma(i)} \neq \infty$ pro $1 \leq i \leq n-k$, pak se jedná o součin Vandermondovy matice, jejíž determinant je roven $\prod_{(i,j):1\leq i<j\leq n-k}(\alpha_{\sigma(j)} - \alpha_{\sigma(i)})$, a diagonální matice, jejíž determinant je roven $v_{\sigma(1)} \ldots v_{\sigma(n-k)}$. Protože prvky α_i, $1 \leq i \leq n$, jsou po dvou různé a prvky $v_{\sigma(1)}, \ldots, v_{\sigma(n-k)}$ jsou všechny nenulové, determinant součinu těchto matic je nenulový, a součin matic je tedy maticí regulární.

Pokud $\alpha_{\sigma(i)} = \infty$ pro nějaké $i \in \{1, \ldots, n-k\}$, použijeme k výpočtu determinantu první matice součinu rozvoj podle i-tého sloupce, čímž přejdeme k výpočtu determinantu Vandermondovy matice $(n-k-1) \times (n-k-1)$, který je opět nenulový. I v tomto případě máme tedy matici regulární.

❑

Dále budeme předpokládat $k, n \in \mathbb{N}$ taková, že $2 \leq k \leq n-2$, $\alpha_1, \ldots, \alpha_n \in F_\infty$ taková, že $\alpha_i \neq \alpha_j$ pro $i \neq j$ a $s = n - k - 1$. Označíme $\boldsymbol{H}(\alpha_1, \ldots, \alpha_n)$ matici

$$\begin{pmatrix} \alpha_1^0 & \alpha_2^0 & \ldots & \alpha_n^0 \\ \alpha_1^1 & \alpha_2^1 & \ldots & \alpha_n^1 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^s & \alpha_2^s & \ldots & \alpha_n^s \end{pmatrix},$$

kde pro $\alpha_i = \infty$ je i-tý sloupec tvaru $(0, \ldots, 0, 1)^\top$ a pro $\alpha_i = 0$ tvaru $(1, 0, \ldots, 0)^\top$.

Tvrzení 2.5. *Pro každou lineární lomenou transformaci $\phi \in \boldsymbol{PGL}(2, F)$ existují čtvercové regulární matice $\boldsymbol{\Phi}$ a $\boldsymbol{D}$ nad F, kde $\boldsymbol{D}$ je diagonální, takové, že*

$$\boldsymbol{\Phi}\boldsymbol{H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{D} = \boldsymbol{H}(\phi(\alpha_1), \ldots, \phi(\alpha_n)).$$

Důkaz. Podle lemmatu 1.6 stačí ukázat existence $\boldsymbol{\Phi}$ a $\boldsymbol{D}$ v případě, kdy $\phi(x) = ax + b$ a kdy $\phi(x) = 1/x$.

Nejdříve ukážeme, jak nalezneme $\boldsymbol{\Phi}$ a $\boldsymbol{D}$, když $\phi(x) = ax + b$. Nechť $a \in F^*$ a $b \in F$. Označme $\boldsymbol{\Phi} = (\phi_{ij})$, $i, j \in \{0, \ldots, s\}$, matici, kde $\phi_{ij} \in F$ jsou daná vztahem

$$(ax + b)^i = \sum_{j=0}^{s} \phi_{ij} x^j.$$

Tato matice je zjevně trojúhelníková, a tedy regulární.

Dále zvolme $\boldsymbol{D} = (d_{ij})$, $i, j \in \{1, \ldots, n\}$, diagonální matici, kde

$$d_{ii} = \begin{cases} 1, & \alpha_i \neq \infty \\ a^{-s}, & \alpha_i = \infty \end{cases}.$$

Pak platí

$$\boldsymbol{\Phi}\boldsymbol{H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{D} = \boldsymbol{H}(a\alpha_1 + b, \ldots, a\alpha_n + b),$$

neboť prvek na pozici i, j $(0 \leq i \leq s,\ 1 \leq j \leq n)$ v matici $\boldsymbol{\Phi}\boldsymbol{H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{D}$ bude roven

$$\sum_{k=0}^{s} \phi_{ik} \alpha_j^k d_{jj} = d_{jj}(a\alpha_j + b)^i;$$

$$d_{jj}(a\alpha_j + b)^i = \begin{cases} (a\alpha_j + b)^i, & \alpha_j \neq \infty \\ a^{-s}(a\alpha_j + b)^i, & \alpha_j = \infty \end{cases};$$

a pro $\alpha_j = \infty$

$$(a\alpha_j + b)^i = \sum_{k=0}^{s} \phi_{ik} \alpha_j^k = \begin{cases} 0, & i < s \\ a^s, & i = s \end{cases}.$$

V případě, že $\phi(x) = 1/x$, položíme

$$\boldsymbol{\Phi} = \begin{pmatrix} 0 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \ldots & 0 \\ 1 & 0 & \ldots & 0 \end{pmatrix}_{(s+1)\times(s+1)}$$

a diagonální prvky matice $\boldsymbol{D}$

$$d_{ii} = \begin{cases} \alpha_i^{-s}, & \alpha_i \neq 0, \infty \\ 1, & \alpha_i = 0, \infty \end{cases}.$$

Potom platí

$$\boldsymbol{\Phi H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{D} = \boldsymbol{H}(1/\alpha_1, \ldots, 1/\alpha_n),$$

protože prvek v matici $\boldsymbol{\Phi H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{D}$ na pozici i, j $(0 \leq i \leq s,\ 1 \leq j \leq n)$ bude roven

$$d_{jj}\alpha_j^{s-i} = \begin{cases} \alpha_j^{-i} = (\frac{1}{\alpha_j})^i, & \alpha_j \neq 0, \infty \\ \alpha_j^{s-i}, & \alpha_j = 0, \infty \end{cases},$$

pro $\alpha_j = 0$

$$\alpha_j^{s-i} = \begin{cases} 0, & i \neq s \\ 1, & i = s \end{cases}$$

a pro $\alpha_j = \infty$

$$\alpha_j^{s-i} = \begin{cases} 0, & i \neq 0 \\ 1, & i = 0 \end{cases}.$$

Vidíme tedy, že j-tý sloupec matice $\boldsymbol{\Phi H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{D}$ bude pro $\alpha_j \neq 0, \infty$ tvaru $(1, 1/\alpha_j, 1/{\alpha_j}^2, \ldots, 1/{\alpha_j}^s)^\top$, pro $\alpha_j = 0$ bude tvaru $(0, \ldots, 0, 1)^\top$ a pro $\alpha_j = \infty$ tvaru $(1, 0, \ldots, 0)^\top$, což odpovídá j-tému sloupci matice $\boldsymbol{H}(1/\alpha_1, \ldots, 1/\alpha_n)$.

❑

Nyní zde uvedeme důsledek, jehož význam bude osvětlen ve čtvrté kapitole.

Důsledek 2.6. *Je-li*

$$\boldsymbol{B} = \boldsymbol{M H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{V},$$

kde $\boldsymbol{M}$ je regulární matice nad F, $\boldsymbol{V}$ je regulární diagonální matice nad F a $\phi \in \boldsymbol{PGL}(2, F)$, pak existují čtvercové regulární matice $\boldsymbol{\Phi}$ a $\boldsymbol{D}$ nad F, kde $\boldsymbol{D}$ je diagonální, takové, že

$$\boldsymbol{B} = \boldsymbol{M\Phi}^{-1}\boldsymbol{H}(\phi(\alpha_1), \ldots, \phi(\alpha_n))\boldsymbol{D}^{-1}\boldsymbol{V}.$$

Důkaz. Z tvrzení 2.5 víme, že existují čtvercové regulární matice $\boldsymbol{\Phi}$ a $\boldsymbol{D}$ nad F, kde $\boldsymbol{D}$ je diagonální, takové, že $\boldsymbol{\Phi H}(\alpha_1, \ldots, \alpha_n)\boldsymbol{D} = \boldsymbol{H}(\phi(\alpha_1), \ldots, \phi(\alpha_n))$. Po vynásobení obou stran rovnosti maticí $\boldsymbol{\Phi}^{-1}$ zleva a maticí $\boldsymbol{D}^{-1}$ zprava dostaneme

$$\boldsymbol{H}(\alpha_1, \ldots, \alpha_n) = \boldsymbol{\Phi}^{-1}\boldsymbol{H}(\phi(\alpha_1), \ldots, \phi(\alpha_n))\boldsymbol{D}^{-1},$$

a proto také

$$\boldsymbol{B} = \boldsymbol{M\Phi}^{-1}\boldsymbol{H}(\phi(\alpha_1), \ldots, \phi(\alpha_n))\boldsymbol{D}^{-1}\boldsymbol{V}.$$

❑

2.3 Dekódování GRS kódů

Zastavme se ještě na chvíli u problému dekódování GRS kódů. Dekódovací algoritmy vždy vycházejí z kanonické prověrkové matice kódu. Jeden z efektivních algoritmů pro dekódování spočívá ve spočítání syndromu a sestavení a vyřešení klíčové rovnice, což vede k nalezení pozicí a hodnot chyb. Nastíníme zde průběh tohoto algoritmu.

Označme $\boldsymbol{H}$ prověrkovou matici GRS kódu z definice 2.12 (pro tento algoritmus budeme potřebovat inverzní prvky k lokátorům). Dále označme $e = (e_1, e_2, \ldots, e_n)$ chybové slovo a J množinu chybových pozic ($e_k \neq 0 \leftrightarrow k \in J$). Předpokládáme, že $|J| \leq \frac{1}{2}(d-1)$. Zavedeme *syndromový polynom*

$$S(x) = \sum_{l=0}^{d-2} S_l x^l, \text{ kde } S_l = \sum_{j \in J} e_j v_j \alpha_j^l,\ l = 0, 1, \ldots, d-2.$$

Vektor $(S_1, \ldots, S_l)$ je tedy právě syndrom přijatého slova. Dále zavedeme *lokalizační polynom*

$$\Lambda(x) = \prod_{j \in J} (1 - \alpha_j x)$$

a *evaluační polynom*

$$\Gamma(x) = \sum_{j \in J} e_j v_j \prod_{m \in J \setminus j} (1 - \alpha_m x).$$

Pro lokalizační polynom platí:

$$\Lambda(\alpha_k^{-1}) = 0 \leftrightarrow k \in J.$$

Z kořenů lokalizačního polynomu tedy poznáme pozice chyb.
Rovnice

$$NSD(\Lambda(x), \Gamma(x)) = 1;$$

$$\deg \Gamma < \deg \Lambda \leq \frac{1}{2}(d-1);$$

$$\Lambda(x) S(x) \equiv \Gamma(x) \pmod{x^{d-1}}$$

tvoří tzv. *klíčovou rovnici*. K jejímu vyřešení lze použít Gaussovu eliminaci (kubická časová složitost) nebo rychlejší Eukleidův či Berlekampův-Masseyův algoritmus (oba kvadratická časová složitost). Takto získáme $\Lambda(x)$ a $\Gamma(x)$. Dále testujeme, zda $\alpha_1^{-1}, \alpha_2^{-1}, \ldots, \alpha_n^{-1}$ jsou kořeny polynomu $\Lambda(x)$ (používá se algoritmus nazvaný Chienovo vyhledávání), a tak získáváme množinu J. Nalezení hodnot chyb je pak už jen otázka vyřešení soustavy lineárních rovnic. Používá se Forneyho algoritmus, což je vlastně vzorec pro výpočet e_k, $k \in J$:

$$e_k = -\frac{\alpha_k}{v_k} \cdot \frac{\Gamma(\alpha_k^{-1})}{\Lambda'(\alpha_k^{-1})},$$

kde $\Lambda'(x) = \sum_{j \in J} (-\alpha_j) \prod_{m \in J \setminus j} (1 - \alpha_m x)$.

Podrobný popis celého algoritmu se zdůvodněním správnosti i popis jednotlivých algoritmů pro řešení klíčové rovnice lze nalézt v [3].

Kapitola 3

McEliecův a Niederreiterův kryptosystém

V roce 1978 představil McEliece asymetrický kryptosystém založený na problému dekódování lineárních kódů [4]. Původní návrh používá binární ireducibilní Goppa kódy. Ukážeme si nyní tento kryptosystém tak, jak je popsán v [5].

Algoritmus 3.1 McEliecův kryptosystém

- **Parametry:** $n, t \in \mathbb{N}$, kde $t \ll n$; lineární $[n, k, d]_q$ kód $\mathcal{C}$ nad $\mathbb{F}_q$, který opraví až t chyb a pro který známe efektivní dekódovací algoritmus $\mathcal{D}_\mathcal{C}$
- **Generování klíčů:**
  $\boldsymbol{S}$: $k \times k$ náhodná regulární matice nad $\mathbb{F}_q$
  $\boldsymbol{G}$: $k \times n$ generující matice kódu $\mathcal{C}$
  $\boldsymbol{P}$: $n \times n$ náhodná permutační matice
  $\boldsymbol{G}^{pub}$: $k \times n$ matice $\boldsymbol{G}^{pub} = \boldsymbol{SGP}$
- **Veřejný klíč:** $(\boldsymbol{G}^{pub}, t)$
- **Soukromý klíč:** $(\boldsymbol{S}, \boldsymbol{G}, \boldsymbol{P})$
- **Šifrování:** Máme zprávu $m \in \mathbb{F}_q^k$. Dále náhodně zvolíme chybový vektor $e \in \mathbb{F}_q^n$ váhy t a spočítáme šifrový text c:

  $$c = m\boldsymbol{G}^{pub} + e.$$

- **Dešifrování:** Abychom dešifrovali šifrový text c, nejprve spočítáme

  $$c\boldsymbol{P}^{-1} = m\boldsymbol{SG} + e\boldsymbol{P}^{-1}.$$

  Následně použijeme dešifrovací algoritmus $\mathcal{D}_\mathcal{C}$ k nalezení $m\boldsymbol{S}$. Otevřený text m dostaneme výpočtem

  $$m\boldsymbol{S}\boldsymbol{S}^{-1}.$$

Poznámka. Dešifrování funguje, neboť máme

$$c\boldsymbol{P}^{-1} = m\boldsymbol{G}^{pub}\boldsymbol{P}^{-1} + e\boldsymbol{P}^{-1} = m\boldsymbol{S}\boldsymbol{G} + e\boldsymbol{P}^{-1}.$$

Protože $e\boldsymbol{P}^{-1}$ má váhu t (permutační matice ji neovlivní) a kód je schopný opravit t chyb, dekódováním získáme $m\boldsymbol{S}$. Otevřený text pak získáme jako $m = m\boldsymbol{S}\boldsymbol{S}^{-1}$.

Soukromým klíčem kryptosystému je v původním návrhu Goppa kód, který se ukázal být dobrou volbou. V minulých třiceti letech sice došlo k úpravě bezpečnostních parametrů, dodnes však není znám žádný útok, který by byl vážnou hrozbou pro tento kryptosystém za podmínky, že používá Goppa kódy. V [6] Dinh, Moore a Russell ukázali, že McEliecův kryptosystém odolává i známým útokům pomocí kvantových počítačů, a můžeme ho tedy zařadit mezi zástupce post-kvantové kryptografie.

Niederreiterův kryptosystém je obdobou McEliecova kryptosystému zveřejněnou v roce 1986 Haraldem Niederreiterem [7]. Místo generující matice využívá matici prověrkovou a zpráva je nejdříve kódována do chybového vektoru na rozdíl od případu McEliecova kryptosystému, který ji reprezentuje jako kódové slovo. Později bylo ukázáno, že tento kryptosystém je stejně bezpečný jako McEliceův [8].

V původním návrhu použil Niederreiter místo Goppa kódů zobecněné Reed-Solomonovy kódy. V roce 1992 však Sidelnikov a Šestakov ve svém článku [1] ukázali, že použití těchto kódů není bezpečné. Jejich útok bude popsán v další kapitole. Existují i návrhy, jak modifikovat Niederreiterův kryptosystém vytvořený nad GRS kódy. Jeden pochází od E. Gabidulina [9], další od T. Bergera a P. Loidreaua [10]. Proti druhému z nich v roce 2006 navrhl útok C. Wieschebrink [11].

Algoritmus 3.2 Niederreiterův kryptosystém

- **Parametry:** $n, t \in \mathbb{N}$, kde $t \ll n$; lineární $[n, k, d]_q$ kód $\mathcal{C}$ nad $\mathbb{F}_q$, který opraví až t chyb a pro který známe efektivní dekódovací algoritmus $\mathcal{D}_\mathcal{C}$
- **Generování klíčů:**
  $\boldsymbol{M} : (n-k) \times (n-k)$ náhodná regulární matice nad $\mathbb{F}_q$
  $\boldsymbol{H} : (n-k) \times n$ prověrková matice kódu $\mathcal{C}$
  $\boldsymbol{P} : n \times n$ náhodná permutační matice
  $\boldsymbol{H}^{pub}$: $(n-k) \times n$ matice $\boldsymbol{H}^{pub} = \boldsymbol{MHP}$
- **Veřejný klíč:** $(\boldsymbol{H}^{pub}, t)$
- **Soukromý klíč:** $(\boldsymbol{M}, \boldsymbol{H}, \boldsymbol{P})$
- **Šifrování:** Zpráva m je reprezentována jako vektor $e \in \mathbb{F}_q^n$ takový, že $w(e) \leq t$. Šifrový text získáme z e následovně:

  $$s = \boldsymbol{H}^{pub} e^\top.$$

  Šifrování tedy odpovídá výpočtu syndromu.
- **Dešifrování:** Abychom dešifrovali šifrový text s, nejprve spočítáme

  $$\boldsymbol{M}^{-1} s = \boldsymbol{HP} e^\top.$$

  Následně použijeme dešifrovací algoritmus $\mathcal{D}_\mathcal{C}$ a získáme $\boldsymbol{P}e^\top$. Otevřený text e dostaneme výpočtem

  $$e^\top = \boldsymbol{P}^{-1}\boldsymbol{P} e^\top.$$

Poznámka. Dešifrování funguje, neboť máme

$$\boldsymbol{M}^{-1} s = \boldsymbol{M}^{-1}\boldsymbol{H}^{pub} e^\top = \boldsymbol{M}^{-1}\boldsymbol{MHP} e^\top = \boldsymbol{HP} e^\top.$$

Protože $\boldsymbol{P}$ neovlivní váhu e, získáme pomocí $\mathcal{D}_\mathcal{C}$ skutečně slovo $\boldsymbol{P}e^\top$ a vynásobením maticí $\boldsymbol{P}^{-1}$ zleva pak $e^\top$.

Kapitola 4

Strukturální útok na Niederreiterův kryptosystém nad GRS kódy

V předchozí kapitole jsme popsali Niederreiterův kryptosystém. Nyní ukážeme strukturální útok na tento kryptosystém v původní podobě, tedy používající zobecněné Reed-Solomonovy kódy. Tento útok byl popsán v roce 1992 Sidelnikovem a Šestakovem [1].

4.1 Kryptosystém a cíl útoku

Nechť je $F = \mathbb{F}_q$ konečné těleso s q prvky a $F_\infty = \mathbb{F}_q \cup \{\infty\}$. Opět zde budeme uvažovat dodefinovanou aritmetiku z první kapitoly. Dále mějme $k, n \in \mathbb{N}$ taková, že $2 \leq k \leq n-2$ a označme $n-k-1$ jako s.

Nechť $\beta_1, \ldots, \beta_n \in F_\infty$, $\beta_i \neq \beta_j$ pro $i \neq j$ a $w_1, \ldots, w_n \in F^*$. Matici tvaru

$$\begin{pmatrix} w_1\beta_1^0 & w_2\beta_2^0 & \ldots & w_n\beta_n^0 \\ w_1\beta_1^1 & w_2\beta_2^1 & \ldots & w_n\beta_n^1 \\ \vdots & \vdots & \ddots & \vdots \\ w_1\beta_1^s & w_2\beta_2^s & \ldots & w_n\beta_n^s \end{pmatrix}$$

budeme značit jako $\boldsymbol{H}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$.

Pro každý polynom

$$f(x) = \sum_{i=0}^{s} a_i x^i \in F[x],\ \deg(f) \leq s,\ \text{bude dále } f(\infty) = a_s.$$

Tedy pokud $\beta_i = \infty$, odpovídající sloupec matice $\boldsymbol{H}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$ je tvaru $w_i(0, \ldots, 0, 1)^\top$.

Tato matice je kanonickou prověrkovou maticí GRS kódu podle definice 2.13 a my ji nyní využijeme pro tvorbu klíčů Niederreiterova kryptosystému.

Odpovídajícím veřejným klíčem bude matice

$$\boldsymbol{H}^{pub} = \boldsymbol{N}\boldsymbol{H}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)\boldsymbol{P},$$

kde $\boldsymbol{N} = (n_{ij})$ je regulární matice nad F typu $(s+1) \times (s+1)$ a $\boldsymbol{P}$ je permutační matice typu $n \times n$. Soukromým klíčem jsou matice $\boldsymbol{N}$, $\boldsymbol{H}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$ a $\boldsymbol{P}$. Pokud by se nám podařilo získat z veřejného klíče kanonickou prověrkovou matici GRS kódu, budeme schopni dešifrovat, neboť známe efektivní dekódovací algoritmus, který využívá právě tuto matici.

Poznámka. Matici $\boldsymbol{P}$ nemusíme při útoku uvažovat.

Důkaz. Když vynásobíme matici $\boldsymbol{H}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$ permutační maticí $\boldsymbol{P}$ zprava, obdržíme matici $\boldsymbol{H}(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}; w_{\sigma(1)}, \ldots, w_{\sigma(n)})$, kde σ je permutace odpovídající matici $\boldsymbol{P}$. Dostáváme tedy opět kanonickou prověrkovou matici GRS kódu. Pokud se nám podaří rozložit matici $\boldsymbol{H}^{pub}$ na součin regulární matice $\boldsymbol{M}$ typu $(s+1) \times (s+1)$ a kanonické prověrkové matice GRS kódu $\boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ typu $(s+1) \times n$ (jedním takovým rozkladem je matice $\boldsymbol{N}$ a matice $\boldsymbol{H}(\beta_{\sigma(1)}, \ldots, \beta_{\sigma(n)}; w_{\sigma(1)}, \ldots, w_{\sigma(n)})$), pak už budeme schopni získat otevřený text e ze šifrového textu $t = \boldsymbol{H}^{pub}e^\top = \boldsymbol{M}\boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)e^\top$.

Můžeme totiž postupovat následujícím způsobem: nejprve spočítáme $\boldsymbol{M}^{-1}t = \boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)e^\top$ a pak použijeme známý dešifrovací algoritmus pro GRS kód s kanonickou prověrkovou maticí $\boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$, čímž získáme e.

❑

Naším cílem bude tedy rozložit matici $\boldsymbol{B}$, pro kterou platí

$$\boldsymbol{B} = \boldsymbol{N}\boldsymbol{H}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n),$$

na součin regulární matice typu $(s+1) \times (s+1)$ a kanonické prověrkové matice GRS kódu typu $(s+1) \times n$.

Matici $\boldsymbol{B}$ můžeme zapsat ve tvaru

$$\boldsymbol{B} = \begin{pmatrix} w_1p_0(\beta_1) & w_2p_0(\beta_2) & \ldots & w_np_0(\beta_n) \\ w_1p_1(\beta_1) & w_2p_1(\beta_2) & \ldots & w_np_1(\beta_n) \\ \vdots & \vdots & \ddots & \vdots \\ w_1p_s(\beta_1) & w_2p_s(\beta_2) & \ldots & w_np_s(\beta_n) \end{pmatrix},$$

kde $p_j(x) = \sum_{i=0}^{s} n_{ji}x^i$, $j = 0, \ldots, s$, jsou polynomy nad F. Platí $p_j(\infty) = n_{js}$.

Příklad 4.1. Ukážeme si příklad daných matic. Budeme pracovat nad tělesem $\mathbb{F}_9$. To konstruujeme jako $\mathbb{Z}_3[x]/(x^2+x+2)$. Jeho prvky budeme zapisovat následovně: 0, 1, 2, α, $\alpha+1$, $\alpha+2$, 2α, $2\alpha+1$, $2\alpha+2$. Nyní vytvoříme prověrkovou matici $\boldsymbol{H}$ GRS kódu s délkou 5 a dimenzí 2. Z těchto parametrů plyne:

$$s = n - k - 1 = 5 - 2 - 1 = 3.$$

Zvolme lokátory $\beta_1 = \alpha$, $\beta_2 = 2\alpha$, $\beta_3 = 2$, $\beta_4 = \alpha + 1$, $\beta_5 = 1$;

a dále multiplikátory $w_1 = 2\alpha + 1$, $w_2 = 1$, $w_3 = 2$, $w_4 = 2\alpha + 2$, $w_5 = \alpha$.

Prověrková matice příslušného GRS kódu vypadá následovně:

$$\boldsymbol{H} = \boldsymbol{H}(\alpha, 2\alpha, 2, \alpha{+}1, 1; 2\alpha{+}1, 1, 2, 2\alpha{+}2, \alpha) = \begin{pmatrix} 2\alpha+1 & 1 & 2 & 2\alpha+2 & \alpha \\ 2\alpha+2 & 2\alpha & 1 & 2\alpha+1 & \alpha \\ 2 & 2\alpha+1 & 2 & \alpha & \alpha \end{pmatrix}.$$

Dále zvolíme

$$\boldsymbol{N} = \begin{pmatrix} \alpha+1 & \alpha+2 & 1 \\ 0 & \alpha & 1 \\ 1 & 2 & 2\alpha+2 \end{pmatrix}.$$

Tato matice je regulární, matice k ní inverzní je

$$\boldsymbol{N}^{-1} = \begin{pmatrix} 0 & \alpha+1 & 1 \\ 2 & \alpha & \alpha+1 \\ \alpha & \alpha & 2 \end{pmatrix}.$$

Nyní spočítáme $\boldsymbol{B}$:

$$\boldsymbol{B} = \boldsymbol{N}\boldsymbol{H} = \begin{pmatrix} 2\alpha+2 & 2\alpha+1 & 0 & 2 & 2\alpha+2 \\ 1 & 0 & \alpha+2 & 2 & 1 \\ \alpha & 1 & \alpha+2 & 0 & 2 \end{pmatrix}.$$

Pro ilustraci zápisů prvků v polynomech:

$$p_0(x) = 1x^2 + (\alpha+2)x + (\alpha+1);$$

$$p_1(x) = 1x^2 + \alpha x;$$

$$p_2(x) = (2\alpha+2)x^2 + 2x + 1.$$

Tedy např.:

$$b_{01} = (2\alpha+1)[1(\alpha)^2 + (\alpha+2)(\alpha) + (\alpha+1)1] = 2\alpha+2;$$

$$b_{11} = (2\alpha+1)[1(\alpha)^2 + (\alpha)(\alpha) + 0\cdot 1)] = 1;$$

$$b_{02} = 1[1(2\alpha)^2 + (\alpha+2)(2\alpha) + (\alpha+1)1] = 2\alpha+1.$$

(Řádky matice $\boldsymbol{B}$ indexujeme od 0, sloupce od 1.)

♣

4.2 Působení grupy lineárních lomených transformací na množině řešení

V této části ukážeme, jak spolu souvisí grupa lineárních lomených transformací $\boldsymbol{PGL}(2, F)$ a množina řešení rovnice

$$\boldsymbol{B} = \boldsymbol{Z}\boldsymbol{H}(x_1, \ldots, x_n; y_1, \ldots, y_n), \tag{4.1}$$

kde neznámými jsou $x_1, \ldots, x_n$, $y_1, \ldots, y_n$ a matice $\boldsymbol{Z}$ a $\boldsymbol{B} = (b_{ij})$ je matice typu $(s{+}1){\times}n$, pro kterou platí $\boldsymbol{B} = \boldsymbol{N}\boldsymbol{H}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$, kde $\beta_1, \ldots, \beta_n \in F_\infty$, $\beta_i \neq \beta_j$ pro $i \neq j$, $w_1, \ldots, w_n \in F^*$ a $\boldsymbol{N}$ je regulární matice nad F.

Řešení rovnice (4.1) nemusí být jednoznačné. Ovšem jak nyní ukážeme, pokud je dáno nějaké řešení $\boldsymbol{Z} = \boldsymbol{M}, x_i = \alpha_i, y_i = v_i$, kde $1 \leq i \leq n$, tak hodnoty α_i a v_i určují už matici $\boldsymbol{M}$ jednoznačně.

Označme $\boldsymbol{H'}$ matici $\boldsymbol{H}(\alpha_1, \ldots, \alpha_{s+1}; v_1, \ldots, v_{s+1})$ (tedy matici, jejíž sloupce tvoří prvních $s+1$ sloupců matice $\boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$) a $\boldsymbol{B'}$ matici skládající se z prvních $s+1$ sloupců matice $\boldsymbol{B}$. Matice $\boldsymbol{H'}$ je regulární, protože ji tvoří $s+1$ sloupců prověrkové matice kódu s minimální vzdáleností $s+2$. Můžeme tedy spočítat matici k ní inverzní $(\boldsymbol{H'})^{-1}$. Vynásobením matice $\boldsymbol{B'}$ maticí $(\boldsymbol{H'})^{-1}$ zprava získáme matici $\boldsymbol{M}$.

Řešení rovnice (4.1) budeme dále vyjadřovat pouze pomocí α_i a v_i.

Lemma 4.1. *Označme $\mathcal{S}$ množinu všech řešení*

$$(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n) \in F_\infty^n \times F^{*n}$$

rovnice (4.1). *Je-li $\phi \in \boldsymbol{PGL}(2, F)$, pak pro každé $(\alpha_1, \ldots, \alpha_n;\ v_1, \ldots, v_n) \in \mathcal{S}$ existují $v'_1, \ldots, v'_n \in F^*$ tak, že $(\phi(\alpha_1), \ldots, \phi(\alpha_n); v'_1, \ldots, v'_n) \in \mathcal{S}$.*

Důkaz. Plyne z důsledku 2.6. ❑

Důsledek 4.2. *Položme*

$$\mathcal{X} = \{(\alpha_1, \ldots, \alpha_n) \in F_\infty^n;\ \exists (v_1, \ldots, v_n) \in F^{*n},\ \text{že } (\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n) \in \mathcal{S}\}.$$

Pak $\boldsymbol{PGL}(2, F)$ působí na $\mathcal{X}$.

Důkaz. Zobrazení $* : \boldsymbol{PGL}(2, F) \times \mathcal{X} \to \mathcal{X}$ definujeme předpisem

$$\phi * (\alpha_1, \ldots, \alpha_n) = (\phi(\alpha_1), \ldots, \phi(\alpha_n)).$$

Pak platí

$$\mathrm{id_F} *(\alpha_1, \ldots, \alpha_n) = (\mathrm{id_F}(\alpha_1), \ldots, \mathrm{id_F}(\alpha_n)) = (\alpha_1, \ldots, \alpha_n)$$

a

$$(\phi\psi) * (\alpha_1, \ldots, \alpha_n) = ((\phi\psi)(\alpha_1), \ldots, (\phi\psi)(\alpha_n)) = (\phi(\psi(\alpha_1)), \ldots, \phi(\psi(\alpha_n))) =$$

$$= \phi * (\psi(\alpha_1), \ldots, \psi(\alpha_n)) = \phi * (\psi * (\alpha_1, \ldots, \alpha_n)).$$

Grupa $\boldsymbol{PGL}(2, F)$ tedy působí na $\mathcal{X}$. ❑

Důsledek 4.3. *Existuje řešení rovnice* (4.1) *ve tvaru*

$$(1, 0, \infty, \alpha_4, \ldots, \alpha_n; v_1, \ldots, v_n)$$

kde $\alpha_4, \ldots, \alpha_n \in F \setminus \{0, 1\}$ a $v_1, \ldots, v_n \in F^*$.

Důkaz. Plyne z 3-tranzitivity grupy $\boldsymbol{PGL}(2, F)$ (tvrzení 1.5) a z důsledku 4.2. ❑

Příklad 4.2. Budeme nyní ilustrovat, jak najít řešení v požadovaném tvaru a odpovídající transformaci, když nějaké řešení známe. Použijeme matici z příkladu 4.1. Mějme

$$\boldsymbol{B} = \boldsymbol{NH} = \begin{pmatrix} 2\alpha+2 & 2\alpha+1 & 0 & 2 & 2\alpha+2 \\ 1 & 0 & \alpha+2 & 2 & 1 \\ \alpha & 1 & \alpha+2 & 0 & 2 \end{pmatrix}.$$

Víme, že

$$x_1 = \beta_1 = \alpha,\ x_2 = \beta_2 = 2\alpha,\ x_3 = \beta_3 = 2,\ x_4 = \beta_4 = \alpha+1,\ x_5 = \beta_5 = 1;$$

$$y_1 = w_1 = 2\alpha+1,\ y_2 = w_2 = 1,\ y_3 = w_3 = 2,\ y_4 = w_4 = 2\alpha+2,\ y_5 = w_5 = \alpha;$$

$$\boldsymbol{Z} = \boldsymbol{N} = \begin{pmatrix} \alpha+1 & \alpha+2 & 1 \\ 0 & \alpha & 1 \\ 1 & 2 & 2\alpha+2 \end{pmatrix}$$

je jedno řešení rovnice $\boldsymbol{B} = \boldsymbol{ZH}(x_1, \ldots, x_5; y_1, \ldots, y_5)$.

Chceme najít řešení ve tvaru $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$, kde $\alpha_1 = 1$, $\alpha_2 = 0$, $\alpha_3 = \infty$ a odpovídající matici $\boldsymbol{Z} = \boldsymbol{M}$.

Nejprve nalezneme lineární lomenou transformaci ϕ takovou, že

$$\phi(\alpha) = 1,\ \phi(2\alpha) = 0,\ \phi(2) = \infty.$$

Budeme postupovat podle důkazu tvrzení 1.5. Nalezneme inverzní transformaci ϕ^{-1}, pro kterou platí:

$$\phi^{-1}(1) = \alpha,\ \phi^{-1}(0) = 2\alpha,\ \phi^{-1}(\infty) = 2.$$

Chceme $\mu_2 \in \boldsymbol{PGL}(2, \mathbb{F}_9)$ takové, že platí $\mu_2(\infty) = 2$. Volíme tedy

$$\mu_2(x) = \frac{2x+1}{x} = (x+2) \circ (\frac{1}{x}) \text{ a odtud máme } \mu_2^{-1}(x) = \frac{1}{x+1}.$$

Dále chceme $\nu_{\beta'} \in \boldsymbol{PGL}(2, \mathbb{F}_9)$ takové, že $\nu_{\beta'}(\infty) = \infty$ a $\nu_{\beta'}(0) = \beta'$. Víme, že

$$\beta' = \mu_2^{-1}(2\alpha) = \frac{1}{2\alpha+1} = \alpha+2,$$

a tedy

$$\nu_{\alpha+2}(x) = x + (\alpha+2) \ \text{ a } \ \nu_{\alpha+2}^{-1}(x) = x + (2\alpha+1).$$

Nakonec chceme $\psi_{\gamma'} \in \boldsymbol{PGL}(2, \mathbb{F}_9)$ pro které platí $\psi_{\gamma'}(\infty) = \infty$, $\psi_{\gamma'}(0) = 0$ a $\psi_{\gamma'}(1) = \gamma'$. Spočteme

$$\gamma' = (\nu_{\alpha+2}^{-1}\mu_2^{-1})(\alpha) = \frac{1}{\alpha+1} + (2\alpha+1) = 1,$$

odtud

$$\psi_1(x) = x.$$

A potom

$$\phi^{-1}(x) = (x+2) \circ (\frac{1}{x}) \circ (x + (\alpha+2)) \circ (x).$$

Dopočítáme $\phi(x)$:

$$\phi(x) = (x + (\alpha+2))^{-1} \circ (\frac{1}{x})^{-1} \circ (x+2)^{-1} = (x + (2\alpha+1)) \circ (\frac{1}{x}) \circ (x+1);$$

$$\phi(x) = \frac{(2\alpha+1)x + 2\alpha + 2}{x+1}.$$

Nyní postupně aplikujeme jednotlivé transformace. Budeme postupovat jako v důkazu tvrzení 2.5. Nejprve $\phi_1(x) = x + 1$:
Hledáme matici $\boldsymbol{\Phi}_1 = (\phi_{ij})$, kde $(x+1)^i = \sum_{j=0}^{s} \phi_{ij} x^j$. Dostáváme

$$\boldsymbol{\Phi}_1 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix}, \quad \boldsymbol{\Phi}_1^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

a

$$\boldsymbol{N}' = \boldsymbol{N}\boldsymbol{\Phi}_1^{-1} = \begin{pmatrix} 0 & \alpha & 1 \\ 2\alpha+1 & \alpha+1 & 1 \\ 2\alpha+1 & 2\alpha+1 & 2\alpha+2 \end{pmatrix}.$$

Dále určíme $\beta'_1, \ldots, \beta'_5$ ze vztahu $\beta'_i = \beta_i + 1$:

$$\beta'_1 = \alpha + 1, \quad \beta'_2 = 2\alpha + 1, \quad \beta'_3 = 2 + 1 = 0,$$

$$\beta'_4 = \alpha + 1 + 1 = \alpha + 2, \quad \beta'_5 = 1 + 1 = 2.$$

Pro výpočet w'_i ze vztahu $w'_i = d_{ii}^{-1} w_i$ potřebujeme:

$$d_{ii}^{-1} = d_{ii} = 1; \; w'_i = 1 w_i, \quad i \in \{1, \ldots, 5\}.$$

Nyní víme, že

$$(\alpha+1,\, 2\alpha+1,\, 0,\, \alpha+2,\, 2;\, 2\alpha+1,\, 1,\, 2,\, 2\alpha+2,\, \alpha);$$

$$\boldsymbol{N}' = \begin{pmatrix} 0 & \alpha & 1 \\ 2\alpha+1 & \alpha+1 & 1 \\ 2\alpha+1 & 2\alpha+1 & 2\alpha+2 \end{pmatrix}$$

je také řešením původní rovnice.

Dále aplikujeme transformaci $\phi_2(x) = 1/x$:
Máme

$$\boldsymbol{\Phi}_2 = \boldsymbol{\Phi}_2^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix};$$

$$\boldsymbol{N}'' = \boldsymbol{N}'\boldsymbol{\Phi}_2^{-1} = \begin{pmatrix} 1 & \alpha & 0 \\ 1 & \alpha+1 & 2\alpha+1 \\ 2\alpha+2 & 2\alpha+1 & 2\alpha+1 \end{pmatrix}.$$

Určíme β_i'', $i \in \{1,\dots,5\}$, ze vztahu $\beta_i'' = (\beta_i')^{-1}$:

$$\beta_1'' = (\alpha+1)^{-1} = \alpha, \quad \beta_2'' = (2\alpha+1)^{-1} = \alpha+2, \quad \beta_3'' = (0)^{-1} = \frac{1}{0} = \infty,$$

$$\beta_4'' = (\alpha+2)^{-1} = 2\alpha+1, \quad \beta_5'' = 2^{-1} = 2.$$

Dále platí:

$d_{ii} = (\beta_i')^{-2}$, $\qquad w_i'' = d_{ii}^{-1} w_i'$, $\qquad i \in \{1,2,4,5\}$;

$d_{11} = (\alpha+1)^{-2} = 2\alpha+1$, $\quad w_1'' = (2\alpha+1)^{-1}(2\alpha+1) = (\alpha+2)(2\alpha+1) = 1$;
$d_{22} = (2\alpha+1)^{-2} = 2$, $\quad w_2'' = 2^{-1}\cdot 1 = 2\cdot 1 = 2$;
$d_{44} = (\alpha+2)^{-2} = 2$, $\quad w_4'' = 2^{-1}(2\alpha+2) = 2(2\alpha+2) = \alpha+1$;
$d_{55} = 2^{-2} = 1$, $\quad w_5'' = 1^{-1}\cdot\alpha = 1\cdot\alpha = \alpha$.

A pro $i = 3$:

$d_{33} = 1$, $\quad w_3'' = 1\cdot 2 = 2$.

Další řešení rovnice tedy je:

$$(\alpha,\ \alpha+2,\ \infty,\ 2\alpha+1,\ 2;\ 1,\ 2,\ 2,\ \alpha+1,\ \alpha);$$

$$\boldsymbol{N}'' = \begin{pmatrix} 1 & \alpha & 0 \\ 1 & \alpha+1 & 2\alpha+1 \\ 2\alpha+2 & 2\alpha+1 & 2\alpha+1 \end{pmatrix}.$$

Nakonec aplikujeme $\phi_3(x) = x + (2\alpha+1)$:
Hledáme matici $\boldsymbol{\Phi}_3 = (\phi_{ij})$, kde $(x+(2\alpha+1))^i = \sum_{j=0}^{s} \phi_{ij} x^j$. Dostáváme

$$\boldsymbol{\Phi}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 2\alpha+1 & 1 & 0 \\ 2 & \alpha+2 & 1 \end{pmatrix}; \quad \boldsymbol{\Phi}_3^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ \alpha+2 & 1 & 0 \\ 2 & 2\alpha+1 & 1 \end{pmatrix};$$

$$\boldsymbol{N}''' = \boldsymbol{N}''\boldsymbol{\Phi}_3^{-1} = \begin{pmatrix} \alpha+2 & \alpha & 0 \\ 0 & \alpha & 2\alpha+1 \\ 2 & 2\alpha & 2\alpha+1 \end{pmatrix}.$$

Určíme $\beta_1''', \dots, \beta_5'''$ ze vztahu $\beta_i''' = \beta_i'' + (2\alpha+1)$:

$$\beta_1''' = \alpha+(2\alpha+1) = 1, \quad \beta_2''' = (\alpha+2)+(2\alpha+1) = 0, \quad \beta_3''' = \infty+(2\alpha+1) = \infty,$$

$$\beta_4''' = (2\alpha+1)+(2\alpha+1) = \alpha+2, \quad \beta_5''' = 2+(2\alpha+1) = 2\alpha.$$

Dále:

$$d_{ii} = d_{ii}^{-1} = 1,\ w_i''' = w_i'', \quad i \in \{1,\dots,5\}.$$

A dostáváme další řešení původní rovnice, a to řešení v námi požadovaném tvaru:

$$(1,\ 0,\ \infty,\ \alpha+2,\ 2\alpha;\ 1,\ 2,\ 2,\ \alpha+1,\ \alpha);$$

$$\boldsymbol{N}''' = \begin{pmatrix} \alpha+2 & \alpha & 0 \\ 0 & \alpha & 2\alpha+1 \\ 2 & 2\alpha & 2\alpha+1 \end{pmatrix}.$$

♣

4.3 Nalezení $\alpha_1, \ldots, \alpha_n$

I nadále předpokládáme $k, n \in \mathbb{N}$, $2 \leq k \leq n-2$ a $s = n-k-1$ a značíme $\boldsymbol{B} = (b_{ij})$ matici $\boldsymbol{NH}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$ typu $(s+1) \times n$, kde $\beta_1, \ldots, \beta_n \in F_\infty$, $\beta_i \neq \beta_j$ pro $i \neq j$, $w_1, \ldots, w_n \in F^*$ a $\boldsymbol{N}$ je regulární matice nad F.

Lemma 4.4. *Matice $\boldsymbol{B}$ je prověrkovou maticí lineárního $[n, n-s-1]$ kódu a zároveň generující maticí lineárního $[n, s+1]$ kódu (označme ho $\mathcal{C}$), jehož kódová slova jsou tvaru*

$$(v_1 g(\alpha_1), v_2 g(\alpha_2), \ldots, v_n g(\alpha_n)),$$

kde $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ je řešením rovnice (4.1) a kde g je polynom nad F stupně nejvýše s (každý takový polynom pak určuje právě jedno kódové slovo kódu $\mathcal{C}$).

Polynom g budeme nazývat *polynomem příslušejícím slovu $c \in \mathcal{C}$ vzhledem k řešení* $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$.

Důkaz. Matice $\boldsymbol{B} = \boldsymbol{NH}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$ je maticí veřejného klíče Niederreiterova kryptosystému využívajícího GRS kód. Dále víme, že $\alpha_1, \ldots, \alpha_n \in F_\infty$ a $v_1, \ldots, v_n \in F^*$ jsou řešením rovnice (4.1). Tedy pro nějakou regulární matici $\boldsymbol{M} = (m_{ij})_{(s+1)\times(s+1)}$ nad F je

$$\boldsymbol{B} = \boldsymbol{MH}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n).$$

Dále víme, že matice $\boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ je prověrkovou maticí lineárního $[n, n-s-1]$ kódu (konkrétně GRS kódu). Když tuto matici vynásobíme regulární maticí $\boldsymbol{M}$, její nulový prostor se nezmění, a matice $\boldsymbol{B}$ bude tedy také prověrkovou maticí lineárního $[n, n-s-1]$ kódu (se stejnou množinou kódových slov). Zároveň tato matice generuje duální $[n, s+1]$ kód, který jsme nazvali $\mathcal{C}$.

Matici $\boldsymbol{B}$ můžeme zapsat ve tvaru

$$\boldsymbol{B} = \begin{pmatrix} v_1 f_0(\alpha_1) & v_2 f_0(\alpha_2) & \ldots & v_n f_0(\alpha_n) \\ v_1 f_1(\alpha_1) & v_2 f_1(\alpha_2) & \ldots & v_n f_1(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ v_1 f_s(\alpha_1) & v_2 f_s(\alpha_2) & \ldots & v_n f_s(\alpha_n) \end{pmatrix},$$

kde $f_j(x) = \sum_{i=0}^{s} m_{ji} x^i$, $j = 0, \ldots, s$, jsou polynomy lineárně nezávislé nad F (množina vektorů jejich koeficientů je lineárně nezávislá). Platí $f_j(\infty) = m_{js}$.

Odtud již vidíme, že kódové slovo kódu generovaného touto maticí bude tvaru

$$(v_1 g(\alpha_1), v_2 g(\alpha_2), \ldots, v_n g(\alpha_n)),$$

kde g bude polynom nad F stupně nejvýše s.

Definujme zobrazení $\mu : F^{s+1} \to F[x]_{s+1}$, kde $F[x]_{s+1}$ je množina všech polynomů jedné proměnné nad F stupně nejvýše s, dané předpisem

$$(u_0, \ldots, u_s) \mapsto \sum_{i=0}^{s} u_i f_i,$$

kde f_i jsou polynomy z matice $\boldsymbol{B}$. Vektor $(u_0, \ldots, u_s)$ odpovídá slovu, které chceme kódovat, výsledný polynom je pak polynomem příslušejícím odpovídajícímu kódovému slovu vzhledem k řešení $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$. Toto zobrazení je prosté díky lineární nezávislosti polynomů f_i, dále $|F^{s+1}| = |F[x]_{s+1}|$, a zobrazení je tedy i na.

Dále definujme zobrazení $\nu : F[x]_{s+1} \to \mathcal{C}$ dané předpisem

$$g \mapsto (v_1 g(\alpha_1), v_2 g(\alpha_2), \ldots, v_n g(\alpha_n)).$$

Abychom dokázali, že zobrazení je prosté, stačí ukázat, že pro každý nenulový polynom g bude existovat $i \in \{1, \ldots, n\}$ takové, že $v_i g(\alpha_i) \neq 0$. Polynom g je stupně nejvýše s, a bude tedy mít nejvýše s kořenů. Z předpokladů na začátku podkapitoly dostáváme, že $s \leq n - 3$. Navíc pokud by bylo $\alpha_j = \infty$ pro nějaké $j \in \{1, \ldots, n\}$ a $g(\alpha_j) = 0$, pak by g byl polynom stupně menšího než s a měl by méně než s kořenů. Můžeme si tedy být jisti, že existuje $i \in \{1, \ldots, n\}$ takové, že $g(\alpha_i) \neq 0$. A protože $v_i \neq 0$, i $v_i g(\alpha_i) \neq 0$. Zobrazení ν je tedy prosté. Zároveň je i na, protože $|\mathcal{C}| = |F[x]_{s+1}| = q^{s+1}$. Jedná se tedy opět o bijekci. Zobrazení $\mu \circ \nu$ bude také bijekce.

To znamená, že každý polynom nad F stupně nejvýše s určuje právě jedno kódové slovo.

❑

Lemma 4.5. *Buď J libovolná podmnožina množiny $\{1, 2, \ldots, n\}$ taková, že $|J| = s$. Z matice $\boldsymbol{B}$ lze odvodit kódové slovo $c = (c_1, \ldots, c_n)$, pro které platí $c_i = 0$ pro všechna $i \in J$ a $w(c) = n - s$.*

Navíc je-li $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ nějaké řešení rovnice (4.1), pak polynom příslušející slovu c vzhledem k tomuto řešení je tvaru

$$g(x) = \lambda \prod_{j \in J : \alpha_j \neq \infty} (x - \alpha_j),$$

kde $\lambda \in F^*$, a dále platí $\deg g \leq s$.

Důkaz. Mějme J podmnožinu množiny $\{1, 2, \ldots, n\}$ takovou, že $|J| = s$. Kód $\mathcal{C}$ je kód generovaný maticí $\boldsymbol{B}$. Hledáme slovo $c \in \mathcal{C}$, pro které $c_i = 0$ pro všechna $i \in J$. Toto slovo vznikne kódováním nějakého slova $u = (u_0, \ldots, u_s) \in F^{s+1}$. Bude platit

$$c = u\boldsymbol{B}, \quad \text{po složkách } \; c_j = \sum_{i=0}^{s} u_i b_{ij}, \quad 1 \leq j \leq n.$$

Požadujeme

$$\sum_{i=0}^{s} u_i b_{ij} = 0 \;\text{ pro } j \in J,\; u_i \neq 0 \text{ pro nějaké } i \in \{0, \ldots, s\}.$$

Tím dostáváme homogenní soustavu s lineárních rovnic o $s+1$ neznámých. Tato soustava má netriviální řešení. Obdržíme tedy slovo $u = (u_0, \ldots, u_s)$ a z něj už snadno dopočítáme kódové slovo $c = (c_1, \ldots, c_n)$.

Nyní předpokládáme, že $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ je řešení rovnice (4.1). To jednoznačně určuje matici $\boldsymbol{M} = (m_{ij})$ takovou, že $\boldsymbol{B} = \boldsymbol{MH}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$.

Podíváme se na polynom příslušející slovu c vzhledem k danému řešení. Ten bude tvaru

$$g(x) = \sum_{i=0}^{s} u_i f_i(x),$$

kde $f_i(x) = \sum_{k=0}^{s} m_{ik} x^k$, $i = 0, \ldots, s$.

Víme, že

$$c_j = \sum_{i=0}^{s} u_i v_j f_i(\alpha_j) = v_j g(\alpha_j)$$

a že v_j jsou všechna nenulová. Proto pro každé $j \in J, \alpha_j \neq \infty$, je α_j kořenem polynomu g. Dále víme, že $\deg g \leq s$, protože $\deg f_i \leq s$. Pokud pro nějaké $j \in J$ je $\alpha_j = \infty$, tj. $g(\alpha_j) = g(\infty) = 0$, pak $\deg g < s$. Tedy

$$g(x) = \lambda \prod_{j \in J: \alpha_j \neq \infty} (x - \alpha_j), \text{ kde } \lambda \in F^*;$$

$$g(\alpha_j) \neq 0, \text{ a tedy } c_j \neq 0 \text{ pro } j \notin J.$$

Odtud máme $w(c) = n - |J| = n - s$.

❑

Důsledek 4.6. *Nechť $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ je řešení rovnice (4.1) takové, že $\alpha_1, \alpha_2 \in F$. Z matice $\boldsymbol{B}$ lze odvodit dvojici slov $c_i \in \mathcal{C}, i \in \{1, 2\}$, jimž příslušející polynomy vzhledem k řešení $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ budou tvaru*

$$g_i(x) = \lambda_i (x - \alpha_i) h(x),$$

kde $\lambda_i \in F^*$, $i \in \{1, 2\}$ a $h(x)$ je polynom nad F, $\deg h \leq s - 1$.

Důkaz. Stačí vzít množiny J_1, J_2 takové, že $J_1 = \{1\} \cup K, J_2 = \{2\} \cup K$, kde $K \subseteq \{3, 4, \ldots, n\}$ taková, že $|K| = s-1$, a postupovat podle důkazu lemmatu 4.5.

❑

Nyní předvedeme, jak najít $\alpha_1, \ldots, \alpha_n \in F_\infty$ taková, že rovnice

$$\boldsymbol{B} = \boldsymbol{ZH}(\alpha_1, \ldots, \alpha_n; y_1, \ldots, y_n),$$

kde neznámými jsou $y_1, \ldots, y_n$ a matice $\boldsymbol{Z}$ a $\boldsymbol{B} = (b_{ij})$ je matice typu $(s+1) \times n$, pro kterou platí $\boldsymbol{B} = \boldsymbol{NH}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n)$, kde $\beta_1, \ldots, \beta_n \in F_\infty$, $\beta_i \neq \beta_j$ pro $i \neq j$, $w_1, \ldots, w_n \in F^*$ a $\boldsymbol{N}$ je regulární matice nad F, má řešení.

Z důsledku 4.3 víme, že existuje řešení rovnice (4.1) $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$, pro které je $\alpha_1 = 1$, $\alpha_2 = 0$ a $\alpha_3 = \infty$. Řešení v tomto tvaru budeme hledat. Máme tedy $\alpha_1 = 1$, $\alpha_2 = 0$ a $\alpha_3 = \infty$.

Z lemmatu 4.4 dále dostáváme, že matice $\boldsymbol{B}$ je generující maticí kódu $\mathcal{C}$ s kódovými slovy tvaru

$$(v_1 g(1), v_2 g(0), v_3 g(\infty), v_4 g(\alpha_4), \ldots, v_n g(\alpha_n)),$$

kde g je polynom nad F stupně nejvýše s.

Nyní využijeme důsledku 4.6. Najdeme slova $c_1, c_2 \in \mathcal{C}$, jimž příslušející polynomy vzhledem k řešení $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ jsou tvaru

$$g_i(x) = \lambda_i(x - \alpha_i)h(x), \quad i \in \{1, 2\},$$

v našem případě tedy

$$g_1(x) = \lambda_1(x - 1)h(x) \quad \text{a} \quad g_2(x) = \lambda_2 x h(x).$$

Zvolme nejdříve množinu K. Z předpokladů víme, že $s \geq 1$. Pokud $s = 1$, pak $K = \emptyset$. Pokud $s \geq 2$, pak zvolíme K jako množinu $\{4, \ldots, s + 2\}$. (Pokud $s = 2$, $K = \{4\}$). Dále předpokládejme $K = \{4, \ldots, s + 2\}$, tedy $s > 1$. Vezměme $J_1 = \{1\} \cup K$ a $J_2 = \{2\} \cup K$.

Nalezením netriviálního řešení soustav

$$\sum_{i=0}^{s} u_{1,i} b_{ij} = 0 \ \text{ pro } j \in J_1$$

a

$$\sum_{i=0}^{s} u_{2,i} b_{ij} = 0 \ \text{ pro } j \in J_2$$

získáme slova $u_1 = (u_{1,0}, \ldots, u_{1,s})$, $u_2 = (u_{2,0}, \ldots, u_{2,s})$, z nichž dopočítáme kódová slova $c_1 = (c_{1,1}, \ldots, c_{1,n})$, $c_2 = (c_{2,1}, \ldots, c_{2,n})$ ze vztahů

$$c_{1,j} = \sum_{i=0}^{s} u_{1,i} b_{ij}, \quad 1 \leq j \leq n,$$

a

$$c_{2,j} = \sum_{i=0}^{s} u_{2,i} b_{ij}, \quad 1 \leq j \leq n.$$

Polynomy příslušející c_1, c_2 vzhledem k řešení $(1, 0, \infty, \alpha_4, \ldots, \alpha_n; v_1, \ldots, v_n)$ budou tvaru

$$g_1(x) = \lambda_1(x - 1)(x - \alpha_4) \ldots (x - \alpha_{s+2})$$

a

$$g_2(x) = \lambda_2 x(x - \alpha_4) \ldots (x - \alpha_{s+2}).$$

Víme, že $c_{1,j} \neq 0$ pro $j = 2, 3, s + 3, \ldots, n$ a $c_{2,j} \neq 0$ pro $j = 1, 3, s + 3, \ldots, n$. Můžeme tedy spočítat

$$t_j = \frac{c_{1,j}}{c_{2,j}}$$

pro $j = 3, s + 3, \ldots, n$. Pro $j = s + 3, \ldots, n$ dostáváme

$$t_j = \frac{v_j g_1(\alpha_j)}{v_j g_2(\alpha_j)} = \frac{\lambda_1(\alpha_j - 1)(\alpha_j - \alpha_4) \ldots (\alpha_j - \alpha_{s+2})}{\lambda_2 \alpha_j (\alpha_j - \alpha_4) \ldots (\alpha_j - \alpha_{s+2})} = \frac{\lambda_1(\alpha_j - 1)}{\lambda_2 \alpha_j}.$$

Pro $t = 3$ je

$$t_3 = \frac{c_{1,3}}{c_{2,3}} = \frac{v_3 g_1(\infty)}{v_3 g_2(\infty)} = \frac{\lambda_1}{\lambda_2}.$$

Úpravou těchto rovnic dostáváme

$$t_j = t_3 \frac{\alpha_j - 1}{\alpha_j}$$

a odtud dále

$$\alpha_j = \frac{t_3}{t_3 - t_j} \quad \text{pro } j = s+3, \ldots, n.$$

K určení α_j, $j = 4, \ldots, s+2$, můžeme použít stejný postup. Vždy najdeme dvojici kódových slov c_1, $c_2 \in \mathcal{C}$, která budou mít na $s-1$ shodných pozicích nuly, dále bude $c_{1,1} = 0$, $c_{2,2} = 0$, $c_{1,3} \neq 0$ a $c_{2,3} \neq 0$ a nakonec $c_{1,i} \neq 0, c_{2,i} \neq 0$, kde α_i chceme určit. Poté spočítáme $t_3 = c_{1,3}/c_{2,3}$, $t_i = c_{1,i}/c_{2,i}$ a α_i získáme ze vztahu $\alpha_i = t_3/(t_3 - t_i)$.

(Pro $s = 1$ bychom postupovali stejně. Polynomy příslušející c_1, c_2 vzhledem k řešení $(1, 0, \infty, \alpha_4, \ldots, \alpha_n; v_1, \ldots, v_n)$ by byly tvaru

$$g_1(x) = \lambda_1(x - 1) \quad \text{a} \quad g_2(x) = \lambda_2 x$$

a opět bychom dostali

$$\alpha_j = \frac{t_3}{t_3 - t_j} \quad \text{pro } j = s+3, \ldots, n.)$$

Vzhledem k tomu, že v parametrech Niederreiterova kryptosystému uvažujeme lineární $[n, k, d]_q$ kód $\mathcal{C}$ nad $\mathbb{F}_q$, který opraví až t chyb, kde $t \ll n$, dále víme, že minimální vzdálenost tohoto kódu je nejmenší d takové, že $2t < d$ ([3]; Tvrzení 1.3), a navíc $d = s + 2$, můžeme předpokládat $2s < n$. Potom nám k získání všech α_j, $j = 1, \ldots, n$, stačí vhodně zvolit pouze dvě dvojice kódových slov, jak to udělali Sidelnikov a Šestakov ve svém článku. Tento postup shrneme v následujícím algoritmu.

Algoritmus 4.1 Nalezení $\alpha_1, \ldots, \alpha_n$

Vstup: matice

$$\boldsymbol{B} = (b_{ij})_{(s+1)\times n} = \boldsymbol{NH}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n),$$

kde $\beta_1, \ldots, \beta_n \in F_\infty$, $\beta_i \neq \beta_j$ pro $i \neq j$, $w_1, \ldots, w_n \in F^*$ a $\boldsymbol{N}$ je regulární matice nad F

Výstup: $\alpha_1, \ldots, \alpha_n$ taková, že rovnice $\boldsymbol{B} = \boldsymbol{ZH}(\alpha_1, \ldots, \alpha_n; y_1, \ldots, y_n)$ má řešení

1: Najdi $u_{1,i}, u_{2,i} \in F$, $0 \leq i \leq s$, taková, že platí

$$\sum_{i=0}^{s} u_{1,i} b_{ij} = 0 \text{ pro } j = 1, s+2, \ldots, 2s;$$

$$\sum_{i=0}^{s} u_{2,i} b_{ij} = 0 \text{ pro } j = 2, s+2, \ldots, 2s;$$

a $u_{1,i}, u_{2,i} \neq 0$ pro nějaké $i \in \{0, \ldots, s\}$.

2: Spočítej

$$c_{1,j} = \sum_{i=0}^{s} u_{1,i} b_{ij} \quad \text{a} \quad c_{2,j} = \sum_{i=0}^{s} u_{2,i} b_{ij}$$

pro $j = 3, \ldots, s+1, 2s+1, \ldots, n$.

3: Spočítej

$$t_j = \frac{c_{1,j}}{c_{2,j}} \text{ pro } j = 3, \ldots, s+1, 2s+1, \ldots, n.$$

4: Najdi $u_{3,i}, u_{4,i} \in F$, $0 \leq i \leq s$, taková, že platí

$$\sum_{i=0}^{s} u_{3,i} b_{ij} = 0 \text{ pro } j = 1, 3, \ldots, s+1;$$

$$\sum_{i=0}^{s} u_{4,i} b_{ij} = 0 \text{ pro } j = 2, 3, \ldots, s+1;$$

a $u_{3,i}, u_{4,i} \neq 0$ pro nějaké $i \in \{0, \ldots, s\}$.

5: Spočítej

$$c_{3,j} = \sum_{i=0}^{s} u_{3,i} b_{ij} \quad \text{a} \quad c_{4,j} = \sum_{i=0}^{s} u_{4,i} b_{ij}$$

pro $j = s+2, \ldots, 2s, n$.

6: Spočítej

$$t_j = \frac{c_{4,n} c_{3,j}}{c_{3,n} c_{4,j}} t_n \text{ pro } j = s+2, \ldots, 2s.$$

7: Polož $\alpha_1 = 1$, $\alpha_2 = 0$ a $\alpha_3 = \infty$ a spočítej $\alpha_j = t_3/(t_3 - t_j)$ pro $4 \leq j \leq n$.

Důkaz. V prvních třech krocích hledáme α_j pro $j = 4, \ldots, s+1, 2s+1, \ldots, n$ postupem, který je uveden výše. (Zde potřebujeme předpoklad $2s < n$.) Samotná α_j dopočítáme v 7. kroku.

Ve 4. a 5. kroku algoritmu najdeme dvojici kódových slov $c_{3,j}, c_{4,j}$, která mají nuly tentokrát na pozicích po řadě $j = 1, 3, \ldots, s+1$ a $j = 2, 3, \ldots, s+1$. Jim příslušející polynomy budou

$$g_3(x) = \sum_{i=0}^{s} u_{3,i} f_i(x) \quad \text{a} \quad g_4(x) = \sum_{i=0}^{s} u_{4,i} f_i(x),$$

kde $f_i(x) = \sum_{j=0}^{s} m_{ij} x^j$.

Protože $g_3(\alpha_3) = g_3(\infty) = 0$, koeficient u x^s v g_3 je roven nule, z čehož plyne $\deg g_3 \leq s-1$. Dále víme, že $\alpha_1, \alpha_4, \ldots, \alpha_{s+1}$ jsou kořeny polynomu g_3, a odtud dostáváme

$$g_3(x) = \lambda_3 (x-1)(x-\alpha_4)\ldots(x-\alpha_{s+1}).$$

Ze stejného důvodu jako u polynomu g_3 dostáváme

$$g_4(x) = \lambda_4 x(x-\alpha_4)\ldots(x-\alpha_{s+1}).$$

Pro $j = s+2, \ldots, n$ pak můžeme určit

$$\frac{c_{3,j}}{c_{4,j}} = \frac{v_j g_3(\alpha_j)}{v_j g_4(\alpha_j)} = \frac{\lambda_3(\alpha_j - 1)(\alpha_j - \alpha_4)\ldots(\alpha_j - \alpha_{s+1})}{\lambda_4 \alpha_j (\alpha_j - \alpha_4)\ldots(\alpha_j - \alpha_{s+1})} = \frac{\lambda_3(\alpha_j - 1)}{\lambda_4 \alpha_j}.$$

Tedy pro $j = n$ platí

$$\frac{c_{3,n}}{c_{4,n}} = \frac{\lambda_3(\alpha_n - 1)}{\lambda_4 \alpha_n} = \frac{\lambda_3(\frac{t_3}{t_3 - t_n} - 1)}{\lambda_4 \frac{t_3}{t_3 - t_n}} = \frac{\lambda_3 \frac{t_n}{t_3 - t_n}}{\lambda_4 \frac{t_3}{t_3 - t_n}} = \frac{\lambda_3 t_n}{\lambda_4 t_3}.$$

Odtud

$$\frac{\lambda_3}{\lambda_4} = \frac{c_{3,n} t_3}{c_{4,n} t_n}, \quad \text{a tedy} \quad \frac{c_{3,j}}{c_{4,j}} = \frac{c_{3,n} t_3 (\alpha_j - 1)}{c_{4,n} t_n \alpha_j}.$$

Nyní položme

$$t_j = \frac{c_{4,n} c_{3,j}}{c_{3,n} c_{4,j}} t_n \quad \text{pro } j = s+2, \ldots, 2s.$$

Potom pro tato j

$$t_j = \frac{c_{4,n}}{c_{3,n}} \frac{c_{3,n} t_3 (\alpha_j - 1)}{c_{4,n} t_n \alpha_j} t_n = \frac{t_3(\alpha_j - 1)}{\alpha_j}, \quad \text{a odtud} \quad \alpha_j = \frac{t_3}{t_3 - t_j}.$$

Vztah $\alpha_j = t_3/(t_3 - t_j)$ tedy skutečně platí pro všechna $j \in \{4, \ldots, n\}$ a výše popsaný algoritmus funguje.

❑

Pokud zvolíme $a \in F$ takové, že $a \neq \alpha_j$ pro $j = 1, \ldots, n$, a nahradíme každé α_j hodnotou $1/(a - \alpha_j)$ (tj. aplikujeme lineární lomenou transformaci), získáme nová $\alpha_1, \ldots, \alpha_n$, pro která bude také platit, že rovnice

$$\boldsymbol{B} = \boldsymbol{ZH}(\alpha_1, \ldots, \alpha_n; y_1, \ldots, y_n)$$

má řešení, a navíc bude platit, že $\alpha_j \neq \infty$ pro všechna $j \in \{1, \ldots, n\}$.

Tvrzení 4.7. *Časová složitost algoritmu 4.1 je $O(s^3 + sn)$ operací v F.*

Důkaz. Výpočet $u_{1,i}$, $u_{2,i}$, $u_{3,i}$ a $u_{4,i}$ znamená čtyřikrát vyřešit homogenní soustavu s lineárních rovnic o $s+1$ neznámých. Časová složitost řešení takové soustavy je $O(s^3)$ operací v F. Časová složitost výpočtu $c_{1,j}$ a $c_{2,j}$ je $O(sn)$ operací v F. Výpočet $c_{3,j}$ a $c_{4,j}$ provedeme s časovou složitostí $O(s^2)$ operací v F. Následný výpočet t_j má časovou složitost $O(n)$ operací v F. Dále spočítáme α_j s časovou složitostí $O(n)$ operací v F. Dohromady máme časovou složitost $O(s^3 + sn)$ operací v F.

❑

Příklad 4.3. Uvažujme těleso $\mathbb{F}_9$ a označme $\boldsymbol{B}$ matici

$$\boldsymbol{B} = \begin{pmatrix} \alpha+2 & 2\alpha & 1 & 2 & 2 & 0 & \alpha+2 \\ 2 & 2 & 2\alpha+2 & 0 & \alpha & 2 & 1 \\ \alpha+1 & 1 & 2 & 2\alpha & \alpha+1 & 2 & \alpha+1 \\ 2\alpha & 2\alpha+1 & \alpha & 1 & 2\alpha+1 & \alpha+2 & \alpha \end{pmatrix}.$$

(Tato matice vznikla jako součin regulární matice

$$\boldsymbol{N} = \begin{pmatrix} \alpha & \alpha+1 & 2\alpha & 2 \\ 0 & \alpha+1 & 2 & 2 \\ \alpha+2 & 1 & \alpha & \alpha+2 \\ 2\alpha+2 & 2\alpha+1 & 1 & 0 \end{pmatrix}$$

a prověrkové matice GRS kódu s lokátory po řadě $2, \alpha+1, 2\alpha+2, 2\alpha, 1, \alpha, 2\alpha+1$ a multiplikátory po řadě $\alpha, 2\alpha+2, \alpha+1, \alpha+2, 2\alpha+2, 2\alpha+1, 2$.)
Budeme řešit rovnici

$$\boldsymbol{ZH}(x_1, \ldots, x_7; y_1, \ldots, y_7) = \boldsymbol{B}.$$

Vidíme, že $n = 7, s = 3$. Naším cílem bude najít $\alpha_1, \ldots, \alpha_7$ taková, že rovnice

$$\boldsymbol{ZH}(\alpha_1, \ldots, \alpha_7; y_1, \ldots, y_7) = \boldsymbol{B}$$

má řešení. Položíme $\alpha_1 = 1, \alpha_2 = 0, \alpha_3 = \infty$. Dále najdeme $u_{1,0}, \ldots, u_{1,3}$ řešící soustavu:

$$\begin{aligned} (\alpha+2)u_{1,0} + 2u_{1,1} + (\alpha+1)u_{1,2} + 2\alpha u_{1,3} &= 0 \\ 2u_{1,0} + \alpha u_{1,1} + (\alpha+1)u_{1,2} + (2\alpha+1)u_{1,3} &= 0 \\ 2u_{1,1} + 2u_{1,2} + (\alpha+2)u_{1,3} &= 0. \end{aligned}$$

Získáváme $u_{1,0} = \alpha, u_{1,1} = 0, u_{1,2} = 1, u_{1,3} = 2\alpha + 1$. Vyřešením soustavy

$$\begin{aligned} 2\alpha u_{2,0} + 2u_{2,1} + 1u_{2,2} + (2\alpha+1)u_{2,3} &= 0 \\ 2u_{2,0} + \alpha u_{2,1} + (\alpha+1)u_{2,2} + (2\alpha+1)u_{2,3} &= 0 \\ 2u_{2,1} + 2u_{2,2} + (\alpha+2)u_{2,3} &= 0 \end{aligned}$$

dostáváme $u_{2,0} = \alpha + 1, u_{2,1} = 1, u_{2,2} = 2\alpha + 2, u_{2,3} = \alpha + 1$.

Nyní spočítáme $c_{1,j}, c_{2,j}$ a t_j pro $j = 3, 4, 7$:

$$
\begin{aligned}
c_{1,3} &= \alpha \cdot 1 + 0(2\alpha + 2) + 1 \cdot 2 + (2\alpha + 1)\alpha = 1,\\
c_{1,4} &= \alpha \cdot 2 + 0 \cdot 0 + 1 \cdot 2\alpha + (2\alpha + 1)1 = 1,\\
c_{1,7} &= \alpha(\alpha + 2) + 0 \cdot 1 + 1(\alpha + 1) + (2\alpha + 1)\alpha = \alpha + 1;
\end{aligned}
$$

$$
\begin{aligned}
c_{2,3} &= (\alpha + 1)1 + 1(2\alpha + 2) + (2\alpha + 2)2 + (\alpha + 1)\alpha = \alpha + 2,\\
c_{2,4} &= (\alpha + 1)2 + 1 \cdot 0 + (2\alpha + 2)2\alpha + (\alpha + 1)1 = 1,\\
c_{2,7} &= (\alpha + 1)(\alpha + 2) + 1 \cdot 1 + (2\alpha + 2)(\alpha + 1) + (\alpha + 1)\alpha = \alpha;
\end{aligned}
$$

$$
\begin{aligned}
t_3 &= \tfrac{1}{\alpha+2} = 2\alpha + 1,\\
t_4 &= \tfrac{1}{1} = 1,\\
t_7 &= \tfrac{\alpha+1}{\alpha} = \alpha + 2.
\end{aligned}
$$

Dále najdeme $u_{3,0}, \ldots, u_{3,3}$ řešící soustavu:

$$
\begin{aligned}
(\alpha + 2)u_{3,0} + \quad & 2u_{3,1} + (\alpha + 1)u_{3,2} + 2\alpha u_{3,3} = 0\\
1u_{3,0} + (2\alpha + 2)u_{3,1} + \quad & 2u_{3,2} + \alpha u_{3,3} = 0\\
2u_{3,0} + \quad & 2\alpha u_{3,2} + 1u_{3,3} = 0.
\end{aligned}
$$

Dostáváme $u_{3,0} = 1, u_{3,1} = 2\alpha, u_{3,2} = 2\alpha, u_{3,3} = \alpha$.

Vyřešíme soustavu

$$
\begin{aligned}
2\alpha u_{4,0} + \quad & 2u_{4,1} + 1u_{4,2} + (2\alpha + 1)u_{4,3} = 0\\
1u_{4,0} + (2\alpha + 2)u_{4,1} + \quad & 2u_{4,2} + \alpha u_{4,3} = 0\\
2u_{4,0} + \quad & 2\alpha u_{4,2} + 1u_{4,3} = 0
\end{aligned}
$$

a získáváme $u_{4,0} = 1, u_{4,1} = 0, u_{4,2} = \alpha + 2, u_{4,3} = \alpha + 2$.

Dále určíme $c_{3,j}, c_{4,j}$ pro $j = 5, 6, 7$:

$$
\begin{aligned}
c_{3,5} &= 2 + 2\alpha \cdot \alpha + 2\alpha(\alpha + 1) + \alpha(2\alpha + 1) = 2,\\
c_{3,6} &= 0 + 2\alpha \cdot 2 + 2\alpha \cdot 2 + \alpha(\alpha + 2) = 1,\\
c_{3,7} &= (\alpha + 2) + 2\alpha \cdot 1 + 2\alpha(\alpha + 1) + \alpha \cdot \alpha = 2\alpha + 2;
\end{aligned}
$$

$$
\begin{aligned}
c_{4,5} &= 2 + (\alpha + 2)(\alpha + 1) + (\alpha + 2)(2\alpha + 1) = 2\alpha,\\
c_{4,6} &= 0 + (\alpha + 2)2 + (\alpha + 2)(\alpha + 2) = 2\alpha,\\
c_{4,7} &= (\alpha + 2) + (\alpha + 2)(\alpha + 1) + (\alpha + 2)\alpha = \alpha;
\end{aligned}
$$

Spočítáme

$$t_5 = \frac{t_7 c_{4,7} c_{3,5}}{c_{3,7} c_{4,5}} = \frac{(\alpha + 2)\alpha \cdot 2}{(2\alpha + 2)2\alpha} = 2\alpha + 2$$

a

$$t_6 = \frac{t_7 c_{4,7} c_{3,6}}{c_{3,7} c_{4,6}} = \frac{(\alpha + 2)\alpha}{(2\alpha + 2)2\alpha} = \alpha + 1.$$

Zbývá určit $\alpha_4, \ldots, \alpha_7$. Platí

$$\alpha_j = \frac{t_3}{t_3 - t_j}.$$

Tedy

$$\alpha_4 = \frac{2\alpha+1}{(2\alpha+1)-1} = 2\alpha, \quad \alpha_5 = \frac{2\alpha+1}{(2\alpha+1)-(2\alpha+2)} = \alpha+2,$$

$$\alpha_6 = \frac{2\alpha+1}{(2\alpha+1)-(\alpha+1)} = \alpha, \quad \alpha_7 = \frac{2\alpha+1}{(2\alpha+1)-(\alpha+2)} = 2.$$

Nyní víme, že rovnice $\boldsymbol{B} = \boldsymbol{ZH}(1, 0, \infty, 2\alpha, \alpha+2, \alpha, 2; y_1, \ldots, y_n)$ má řešení.

Položme $a = 2\alpha + 1$ a aplikujme transformaci

$$\phi(x) = \frac{1}{2x+a} = \frac{1}{2x+(2\alpha+1)}.$$

Dostaneme

$$\phi(\alpha_1) = \frac{1}{2+(2\alpha+1)} = 2\alpha+2, \quad \phi(\alpha_2) = \frac{1}{2\cdot 0+(2\alpha+1)} = \alpha+2,$$

$$\phi(\alpha_3) = \frac{1}{2\infty+(2\alpha+1)} = 0, \quad \phi(\alpha_4) = \frac{1}{2(2\alpha)+(2\alpha+1)} = 1,$$

$$\phi(\alpha_5) = \frac{1}{2(\alpha+2)+(2\alpha+1)} = 2\alpha+1, \quad \phi(\alpha_6) = \frac{1}{2\alpha+(2\alpha+1)} = \alpha,$$

$$\phi(\alpha_7) = \frac{1}{2\cdot 2+(2\alpha+1)} = 2\alpha.$$

Existuje tedy i řešení rovnice

$$\boldsymbol{ZH}(2\alpha+2, \alpha+2, 0, 1, 2\alpha+1, \alpha, 2\alpha; y_1, \ldots, y_7) = \boldsymbol{B}.$$

♣

4.4 Nalezení $v_1, \ldots, v_n$ a matice $\boldsymbol{M}$

Už jsme našli $\alpha_1, \ldots, \alpha_n$, kde $\alpha_j \neq \infty$ pro $j = 1, \ldots, n$, taková, že rovnice

$$\boldsymbol{B} = \boldsymbol{ZH}(\alpha_1, \ldots, \alpha_n; y_1, \ldots, y_n), \tag{4.2}$$

kde neznámými jsou $y_1, \ldots, y_n$ a matice $\boldsymbol{Z}$, má řešení.

Víme také, že pokud najdeme nějaká $y_1 = v_1, \ldots, y_n = v_n$, pro která má rovnice

$$\boldsymbol{B} = \boldsymbol{ZH}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$$

řešení $\boldsymbol{Z} = \boldsymbol{M}$, bude toto řešení už jednoznačné.

Nyní ukážeme, jak najdeme řešení rovnice (4.2) s časovou složitostí $O(s^3+sn)$.

Algoritmus 4.2 Nalezení $v_1, \ldots, v_n$ a matice $\boldsymbol{M}$

Vstup: matice

$$\boldsymbol{B} = (b_{ij})_{(s+1)\times n} = \boldsymbol{NH}(\beta_1, \ldots, \beta_n; w_1, \ldots, w_n),$$

kde $\beta_1, \ldots, \beta_n \in F_\infty$, $\beta_i \neq \beta_j$ pro $i \neq j$, $w_1, \ldots, w_n \in F^*$ a $\boldsymbol{N}$ je regulární matice nad F; $\alpha_1, \ldots, \alpha_n$ taková, že $\alpha_j \neq \infty$ pro každé $j \in \{1, \ldots, n\}$ a rovnice $\boldsymbol{B} = \boldsymbol{ZH}(\alpha_1, \ldots, \alpha_n; y_1, \ldots, y_n)$ má řešení

Výstup: regulární matice $\boldsymbol{M} = (m_{ik})_{i,k=0}^{s}$ nad F a $v_1, \ldots, v_n \in F^*$ taková, že

$$\boldsymbol{B} = \boldsymbol{MH}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$$

1: Najdi $c_j \in F, 1 \leq j \leq s+2$, taková, že platí

$$\sum_{j=1}^{s+2} c_j b_{ij} = 0, \quad 0 \leq i \leq s,$$

a $c_j \neq 0$ pro nějaké $j \in \{1, \ldots, s+2\}$.

2: Polož $v_1 = 1$ a najdi $v_2, \ldots, v_{s+2} \in F$ taková, že

$$\sum_{j=1}^{s+2} c_j v_j \alpha_j^i = 0, \quad 0 \leq i \leq s.$$

3: Pro každé i, $0 \leq i \leq s$, najdi $m_{i0}, \ldots, m_{is} \in F$ řešící soustavu

$$\sum_{k=0}^{s} m_{ik} \alpha_j^k = v_j^{-1} b_{ij}, \quad 1 \leq j \leq s+1,$$

a polož $\boldsymbol{M} = (m_{ij})$.

4: Najdi matici $\boldsymbol{M}^{-1} = (m'_{ij})$ a spočítej

$$v_j = \sum_{i=0}^{s} m'_{0i} b_{ij}, \quad s+3 \leq j \leq n.$$

Důkaz. Pokud budou $v_1, \ldots, v_n$ a $\boldsymbol{M} = (m_{ik})_{i,k=0}^{s}$ nějakým řešením rovnice (4.2) a vezmeme $\widetilde{v}_j = a v_j$, kde $j = 1, \ldots, n$ a $a \in F^*$, a matici $\widetilde{\boldsymbol{M}} = (\widetilde{m}_{ik})_{i,k=0}^{s}$, kde $\widetilde{m}_{ik} = a^{-1} m_{ik}$, bude platit

$$\boldsymbol{B} = \boldsymbol{MH}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n) = \widetilde{\boldsymbol{M}} H(\alpha_1, \ldots, \alpha_n; \widetilde{v}_1, \ldots, \widetilde{v}_n)$$

a $\widetilde{v}_1, \ldots, \widetilde{v}_n$ a $\widetilde{\boldsymbol{M}}$ budou také řešit rovnici (4.2).

Existuje tedy řešení rovnice (4.2) $y_1 = v_1, \ldots, y_n = v_n$, $\boldsymbol{Z} = \boldsymbol{M}$, kde $v_1 = 1$. Řešení v tomto tvaru budeme hledat. Položme tedy $v_1 = 1$ a hledejme příslušná $v_2, \ldots, v_n$ a matici $\boldsymbol{M}$.

Soustava

$$\sum_{j=1}^{s+2} c_j b_{ij} = 0, \quad 0 \leq i \leq s,$$

je homogenní soustava $s+1$ lineárních rovnic o $s+2$ neznámých. Má tedy netriviální řešení. Kdyby existovalo $j \in \{1, \ldots, s+2\}$ tak, že $c_j = 0$, pak by matice $\boldsymbol{B}$ obsahovala $s+1$ lineárně závislých sloupců, což neobsahuje (protože GRS kód je MDS kód). Víme tedy, že $c_j \neq 0$ pro $j \in \{1, \ldots, s+2\}$.

Využijeme toho, že matici $\boldsymbol{B}$ můžeme vyjádřit ve tvaru

$$\boldsymbol{B} = \begin{pmatrix} v_1 f_0(\alpha_1) & v_2 f_0(\alpha_2) & \ldots & v_n f_0(\alpha_n) \\ v_1 f_1(\alpha_1) & v_2 f_1(\alpha_2) & \ldots & v_n f_1(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ v_1 f_s(\alpha_1) & v_2 f_s(\alpha_2) & \ldots & v_n f_s(\alpha_n) \end{pmatrix},$$

kde $f_j(x) = \sum_{i=0}^{s} m_{ji} x^i$, $j = 0, \ldots, s$. Dosazením za b_{ij} dostáváme soustavu

$$\sum_{j=1}^{s+2} c_j v_j f_i(\alpha_j) = 0, \quad 0 \leq i \leq s.$$

Tuto soustavu lze zapsat také následujícím způsobem:

$$\begin{pmatrix} f_0(\alpha_1) & f_0(\alpha_2) & \ldots & f_0(\alpha_{s+2}) \\ f_1(\alpha_1) & f_1(\alpha_2) & \ldots & f_1(\alpha_{s+2}) \\ \vdots & \vdots & \ddots & \vdots \\ f_s(\alpha_1) & f_s(\alpha_2) & \ldots & f_s(\alpha_{s+2}) \end{pmatrix} \begin{pmatrix} c_1 & 0 & \ldots & 0 \\ 0 & c_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & c_{s+2} \end{pmatrix} \begin{pmatrix} 1 \\ v_2 \\ \vdots \\ v_{s+2} \end{pmatrix} = 0.$$

Po vynásobení maticí $\boldsymbol{M}^{-1}$ zleva dostáváme:

$$\begin{pmatrix} \alpha_1^0 & \alpha_2^0 & \ldots & \alpha_{s+2}^0 \\ \alpha_1^1 & \alpha_2^1 & \ldots & \alpha_{s+2}^1 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^s & \alpha_2^s & \ldots & \alpha_{s+2}^s \end{pmatrix} \begin{pmatrix} c_1 & 0 & \ldots & 0 \\ 0 & c_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & c_{s+2} \end{pmatrix} \begin{pmatrix} 1 \\ v_2 \\ \vdots \\ v_{s+2} \end{pmatrix} = 0.$$

Tedy platí:

$$\sum_{j=2}^{s+2} c_j \alpha_j^i v_j = -c_1 \alpha_1^i, \quad 0 \leq i \leq s.$$

Jde o soustavu $s+1$ rovnic o $s+1$ neznámých. Tato soustava má jednoznačné řešení, pokud determinant matice soustavy je nenulový. Tak tomu skutečně je, neboť platí

$$\det \begin{pmatrix} c_2\alpha_2^0 & c_3\alpha_3^0 & \ldots & c_{s+2}\alpha_{s+2}^0 \\ c_2\alpha_2^1 & c_3\alpha_3^1 & \ldots & c_{s+2}\alpha_{s+2}^1 \\ \vdots & \vdots & \ddots & \vdots \\ c_2\alpha_2^s & c_3\alpha_3^s & \ldots & c_{s+2}\alpha_{s+2}^s \end{pmatrix} = c_2 c_3 \ldots c_{s+2} \det \begin{pmatrix} \alpha_2^0 & \alpha_3^0 & \ldots & \alpha_{s+2}^0 \\ \alpha_2^1 & \alpha_3^1 & \ldots & \alpha_{s+2}^1 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_2^s & \alpha_3^s & \ldots & \alpha_{s+2}^s \end{pmatrix} \neq 0,$$

protože jde o součin nenulových prvků tělesa s determinantem Vandermondovy matice, který je nenulový, protože $\alpha_i \neq \alpha_j$ pro $i \neq j$. Vyřešením soustavy tedy získáme $v_2, \ldots, v_{s+2}$.

Platí

$$b_{ij} = v_j \sum_{k=0}^{s} m_{ik} \alpha_j^k.$$

Vyřešením soustavy

$$\sum_{k=0}^{s} m_{ik}\alpha_j^k = v_j^{-1}b_{ij}, \quad 1 \le j \le s+1,$$

pro pevné i získáme i-tý řádek matice $\boldsymbol{M}$. Řešení soustavy je opět jednoznačné, neboť determinant soustavy je Vandermondovým determinantem. Vyřešením této soustavy pro každé i, $0 \le i \le s$, získáme celou matici $\boldsymbol{M}$. Všimněme si, že opakovaně řešíme soustavu se stejnou levou stranou, pouze měníme vektor napravo. Bude tedy výhodné řešit soustavu pro všechny pravé strany najednou. Časová složitost tohoto kroku pak odpovídá časové složitosti nalezení inverzní matice.

Zbývá dopočítat $v_{s+3}, \ldots, v_n$. Když vynásobíme matici $\boldsymbol{B}$ maticí $\boldsymbol{M}^{-1}$ zleva, získáme $\boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$. První řádek matice $\boldsymbol{H}(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$ je $(v_1, \ldots, v_n)$. Po spočítání $\boldsymbol{M}^{-1} = (m'_{ij})$ proto snadno dopočítáme zbývající v_j z rovnic

$$v_j = \sum_{i=0}^{s} m'_{0i}b_{ij}, \quad s+3 \le j \le n.$$

❑

Tvrzení 4.8. *Časová složitost algoritmu 4.2 je $O(s^3 + sn)$ operací v F.*

Důkaz. V prvním kroku řešíme homogenní soustavu $s+1$ lineárních rovnic o $s+2$ neznámých. Složitost tohoto výpočtu je $O(s^3)$ operací v F. Ve druhém kroku řešíme soustavu $s+1$ rovnic o $s+1$ neznámých opět se složitostí $O(s^3)$ operací v F (pro vytvoření matice soustavy sestavíme Vandermondovu matici se složitostí $O(s^2)$ operací v F).

Dále spočítáme matici $\boldsymbol{M}$ se složitostí $O(s^3)$ operací v F (vyřešíme soustavu $s+1$ rovnic o $s+1$ neznámých pro několik pravých stran najednou). Opět zde sestavujeme Vandermondovu matici, kterou už ale máme až na jeden sloupec vypočítanou z předchozího kroku. Nalezení inverzní matice a dopočítání zbývajících v_j pak provedeme s časovou složitostí $O(s^3+sn)$ operací v F. Celková složitost algoritmu je tedy $O(s^3 + sn)$ operací v F.

❑

Důsledek 4.9. *Časová složitost nalezení kompletního řešení rovnice*

$$\boldsymbol{B} = \boldsymbol{Z}\boldsymbol{H}(x_1, \ldots, x_n; y_1, \ldots, y_n) \text{ je } O(s^3 + sn) \text{ operací v } F.$$

Příklad 4.4. Budeme pokračovat v řešení rovnice z příkladu 4.3. Známe matici $\boldsymbol{B}$ a již víme, že existuje řešení rovnice (4.1) $(\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n)$, kde $\alpha_1 = 2\alpha + 2$, $\alpha_2 = \alpha + 2$, $\alpha_3 = 0$, $\alpha_4 = 1$, $\alpha_5 = 2\alpha + 1$, $\alpha_6 = \alpha$ a $\alpha_7 = 2\alpha$. Nyní dopočítáme $v_1, \ldots, v_7$ a matici $\boldsymbol{M}$.

Nejdříve najdeme $c_1, \ldots, c_5$ tak, aby

$$\begin{aligned}
(\alpha+2)c_1 + \quad 2\alpha c_2 + \quad 1c_3 + \quad 2c_4 + \quad 2c_5 &= 0\\
2c_1 + \quad 2c_2 + (2\alpha+2)c_3 + \quad \alpha c_5 &= 0\\
(\alpha+1)c_1 + \quad 1c_2 + \quad 2c_3 + 2\alpha c_4 + \quad (\alpha+1)c_5 &= 0\\
2\alpha c_1 + (2\alpha+1)c_2 + \quad \alpha c_3 + \quad 1c_4 + (2\alpha+1)c_5 &= 0.
\end{aligned}$$

Vyřešením soustavy dostaneme $c_1 = 1, c_2 = 2\alpha + 2, c_3 = \alpha, c_4 = \alpha, c_5 = \alpha$. Položíme $v_1 = 1$. Vyřešením soustavy $\sum_{j=1}^{s+2} c_j \alpha_j^i v_j = 0,\ 0 \le i \le s$, tj. soustavy

$$\begin{aligned}
(2\alpha+2)v_2 + \alpha v_3 + \alpha v_4 + \quad \alpha v_5 &= -1 \\
(2\alpha+2)(\alpha+2)v_2 + \quad + \alpha v_4 + \ \alpha(2\alpha+1)v_5 &= -(2\alpha+2) \\
(2\alpha+2)(\alpha+2)^2 v_2 + \quad + \alpha v_4 + \alpha(2\alpha+1)^2 v_5 &= -(2\alpha+2)^2 \\
(2\alpha+2)(\alpha+2)^3 v_2 + \quad + \alpha v_4 + \alpha(2\alpha+1)^3 v_5 &= -(2\alpha+2)^3,
\end{aligned}$$

obdržíme $v_2 = \alpha + 1, v_3 = 2\alpha + 1, v_4 = 2\alpha + 2, v_5 = 2$.

Matici $\boldsymbol{M}$ získáme vyřešením soustavy

$$\begin{aligned}
1m_{i0} + (2\alpha+2)m_{i1} + (\alpha+2)m_{i2} + \quad \alpha m_{i3} &= 1^{-1}b_{i1} \\
1m_{i0} + \ (\alpha+2)m_{i1} + \quad 2m_{i2} + (2\alpha+1)m_{i3} &= (\alpha+1)^{-1}b_{i2} \\
1m_{i0} \qquad\qquad\qquad\qquad\qquad\qquad &= (2\alpha+1)^{-1}b_{i3} \\
1m_{i0} + \quad 1m_{i1} + \quad 1m_{i2} + \quad 1m_{i3} &= (2\alpha+2)^{-1}b_{i4}
\end{aligned}$$

po dosazení příslušných b_{ij} pro $0 \le i \le s$. Dostáváme tak

$$\boldsymbol{M} = \begin{pmatrix} \alpha+2 & 1 & 2\alpha+2 & \alpha+1 \\ \alpha & 0 & 2\alpha & 0 \\ 2\alpha+1 & 2\alpha+2 & 2\alpha & 2\alpha+1 \\ \alpha+1 & 2\alpha+2 & \alpha+2 & \alpha+1 \end{pmatrix}.$$

Matice k ní inverzní je

$$\boldsymbol{M}^{-1} = \begin{pmatrix} 2 & 2\alpha+2 & 2\alpha & 0 \\ 1 & 2\alpha+2 & 2\alpha+1 & \alpha+2 \\ 2 & \alpha+1 & 2\alpha & 0 \\ \alpha & 2\alpha+1 & 2 & 2\alpha+2 \end{pmatrix}.$$

Dopočítáme v_6 a v_7:

$v_6 = (2\alpha+2)2 + 2\alpha \cdot 2 = 2\alpha + 1$,

$v_7 = 2(\alpha+2) + (2\alpha+2) + 2\alpha(\alpha+1) = \alpha + 2$.

Dostali jsme možné řešení rovnice

$$\boldsymbol{ZH}(x_1, \ldots, x_7; y_1, \ldots, y_7) = \boldsymbol{B}.$$

Toto řešení je:

$$(2\alpha+2,\ \alpha+2,\ 0,\ 1,\ 2\alpha+1,\ \alpha,\ 2\alpha; 1,\ \alpha+1,\ 2\alpha+1,\ 2\alpha+2,\ 2,\ 2\alpha+1,\ \alpha+2);$$

$$\boldsymbol{M} = \begin{pmatrix} \alpha+2 & 1 & 2\alpha+2 & \alpha+1 \\ \alpha & 0 & 2\alpha & 0 \\ 2\alpha+1 & 2\alpha+2 & 2\alpha & 2\alpha+1 \\ \alpha+1 & 2\alpha+2 & \alpha+2 & \alpha+1 \end{pmatrix}.$$

♣

Závěr

Těžištěm práce je podrobný popis útoku na Niederreiterův kryptosystém vytvořený nad GRS kódy. Kromě samotného útoku byla v práci také prezentována problematika působení grupy na množině, byla zavedena projektivní lineární grupa a dokázána její 3-tranzitivita. Později bylo ukázáno, že tato grupa úzce souvisí s množinou řešení rovnice (4.1). Konkrétně působí na množině $\mathcal{X} = \{(\alpha_1, \ldots, \alpha_n) \in F_\infty^n; \exists (v_1, \ldots, v_n) \in F^{*n}, \text{ že } (\alpha_1, \ldots, \alpha_n; v_1, \ldots, v_n) \in \mathcal{S}\}$, kde $\mathcal{S}$ je množina řešení rovnice (4.1). Vidíme, že možných $(\alpha_1, \ldots, \alpha_n)$ je stejně jako prvků projektivní lineární grupy, přitom pomocí libovolného řešení rovnice (4.1) jsme schopni dešifrovat. Takových řešení je pak ještě více, než je prvků projektivní lineární grupy, protože pro pevně dané $(\alpha_1, \ldots, \alpha_n)$ není $(v_1, \ldots, v_n)$ dáno jednoznačně. Už takový počet možných řešení ukazuje na určitou slabinu Niederreiterova původního návrhu. Další slabinou se zdá být i to, že permutační matice $\boldsymbol{P}$ nemá v tomto návrhu vlastně žádný význam.

Přínosem práce je podrobné zpracování a zpřehlednění útoku. Zejména bych zmínila pohled na matici $\boldsymbol{B}$ jako na generující matici jistého kódu. Lokátory hledané prověrkové matice GRS kódu pak vlastně určujeme pomocí výpočtu podílů nenulových souřadnic speciálně volených slov tohoto kódu. Dále je přidán podrobný výklad potřebných vlastností projektivní lineární grupy. Je také zpřesněna časová složitost útoku. Autoři původního článku si zřejmě nevšimli, že při výpočtu matice $\boldsymbol{M}$ řeší opakovaně soustavu se stejnou levou stranou, a složitost tohoto kroku pak určili jako $O(s^4)$, přitom lze tento odhad zmenšit na $O(s^3)$. Pro ilustraci byly uvedeny příklady. K výpočtům nad konečnými tělesy byl použit matematický software `Wolfram Mathematica 9`.

Literatura

[1] Sidelnikov V. M., Shestakov S. O. On insecurity of cryptosystems based on generalized Reed–Solomon codes. *Discrete Mathematics and Applications*, 2(4):439–444, 1992.

[2] Macálková L. Akce grupy. Bakalářská práce, Masarykova univerzita, 2009.

[3] Roth Ron M. *Introduction to Coding Theory*. Cambridge University Press, Cambridge, 2006.

[4] McEliece R. J. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 42(44):114–116, 1978.

[5] Overbeck R., Sendrier N. Code-based cryptography. Bernstein D.J., Buchmann J. , Dahmen E., *Post-Quantum Cryptography*, str. 95–145. Springer, 2009.

[6] Dinh H., Moore C., Russell A. McEliece and Niederreiter Cryptosystems That Resist Quantum Fourier Sampling Attacks. *CRYPTO*, str. 761–779, 2011.

[7] Niederreiter H. Knapsack-type cryptosystems and algebraic coding theory. *Probl. Control and Inform. Theory*, 15(2):159–166, 1986.

[8] Li Y., Deng R., Wang X. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, 1994.

[9] Gabidulin E. On public-key cryptosystems based on linear codes. *Proc. of 4th IMA Conference on Cryptography and Coding 1993*. IMA Press, 1995.

[10] Berger T., Loidreau P. How to mask the structure of codes for a cryptographic use. *Designs, Codes and Cryptography*, 35(1):63–79, 2005.

[11] Wieschebrink C. An attack on a modified Niederreiter encryption scheme. *Public Key Cryptography*, str. 14–26, 2006.