MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA
ÚSTAV MATEMATIKY A STATISTIKY

Bakalářská práce

BRNO 2015 **JAN PLHÁK**

MASARYKOVA UNIVERZITA
PŘÍRODOVĚDECKÁ FAKULTA
ÚSTAV MATEMATIKY A STATISTIKY

Název práce na titulní list

Bakalářská práce

Jan Plhák

Vedoucí práce: Bc. Lukáš Vokřínek, PhD. **Brno 2015**

Bibliografický záznam

Autor:	Jan Plhák Přírodovědecká fakulta, Masarykova univerzita Ústav matematiky a statistiky
Název práce:	Název práce
Studijní program:	Matematika
Studijní obor:	Obecná matematika
Vedoucí práce:	Bc. Lukáš Vokřínek, PhD.
Akademický rok:	2014/2015
Počet stran:	?? + ??
Klíčová slova:	Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo; Klíčové slovo

Bibliographic Entry

Author:	Jan Plhák Faculty of Science, Masaryk University Department of Mathematics and Statistics
Title of Thesis:	Title of Thesis
Degree Programme:	Mathematics
Field of Study:	Mathematics
Supervisor:	Bc. Lukáš Vokřínek, PhD.
Academic Year:	2014/2015
Number of Pages:	?? + ??
Keywords:	Keyword; Keyword; Keyword; Keyword; Keyword; Keyword; Keyword; Keyword; Keyword

Abstrakt

V této bakalářské/diplomové/rigorózní práci se věnujeme ...

Abstract

In this thesis we study ...

Místo tohoto listu vložte kopii oficiálního (podepsaného) zadání práce.

Poděkování

Na tomto místě bych chtěl(-a) poděkovat ...

Prohlášení

Prohlašuji, že jsem svoji bakalářskou/diplomovou/rigorózní práci vypracoval(-a) samostatně s využitím informačních zdrojů, které jsou v práci citovány.

Brno xx. měsíce 20xx

. . . . . .

Jan Plhák

Obsah

Úvod

Cílem této práce je seznámit čtenáře s efektivním algoritmem pro výpočet Smithova normálního tvaru celočíselných matic.

Přehled použitého značení

Pro snažší orientaci v textu zde čtenáři předkládáme přehled základního značení, které se v celé práci vyskytuje.

$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel

$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel

$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel
$\mathbb{C}$	množina všech komplexních čísel
$\mathbb{R}$	množina všech reálných čísel
$\mathbb{Z}$	množina všech celých čísel
$\mathbb{N}$	množina všech přirozených čísel

Kapitola 1

Smithův normální tvar

V této kapitole se budeme zbývat definicí Smithova normálního tvaru (budeme značit SNF) celočíselných matic $Mat_{n\times m}\mathbb{Z}$, dokážeme jeho existenci pro libovolnou $A \in Mat_{n\times m}\mathbb{Z}$ a konečně uvedeme souvislost mezi SNF a konečně generovanými komutativními grupami.

Definice 1.1. Řekneme že matice A $\in Mat_{n\times m}\mathbb{Z}$ je ve Smithově normálním tvaru jestliže

$$A = \begin{pmatrix} q_1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & q_2 & \ddots & & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & & \vdots \\ \vdots & & \ddots & q_k & \ddots & & \vdots \\ \vdots & & & \ddots & 0 & \ddots & \vdots \\ \vdots & & & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0 \end{pmatrix}$$

a platí $q_i | q_{i+1}$ kde $i \in \{1,\ldots,k-1\}$. Čísla q_i pak nazýváme *invariantními faktory*.

Věta 1.2 (O Smithově normálním tvaru)**.** *Pro libovolnou celočíselnou matici $B \in Mat_{n\times m}\mathbb{Z}$ existují invertibilní matice $P,Q \in Mat_{n\times m}\mathbb{Z}$ a matice A ve Smithově normálním tvaru takové, že platí*

$$B = P \cdot A \cdot Q$$

Smithův normální tvar je jednoznačný až na znaménka invariantních faktorů.

Než se pustíme do samotného důkazu této věty, je dobré si uvědomit, jak vlastně vypadají invertibilní celočíselné matice. To popisuje následující lemma.

Lemma 1.3. *Buď $A \in Mat_{n\times m}\mathbb{Z}$. Pak je A invertiblní, právě tehdy když je čtvercová a* $\det(A) = \pm 1$.

Důkaz. Buď $A \in Mat_{n\times m}\mathbb{Z}$ invertibilní. Existuje tedy matice $A^{-1} \in Mat_{n\times m}\mathbb{Z}$ taková, že $AA^{-1} = E$. Pak je ovšem A^{-1} inverzí pro A také nad $\mathbb{Q}$. Proto A musí být čtvercová, neboť každá invertiblní matice nad $\mathbb{Q}$ je čtvercová a má nenulový determinant. Navíc platí

$$det(A) \cdot \det(A^{-1}) = det(AA^{-1}) = det(E) = 1$$

a protože determinant celočíselné matice je z definice determinantu také celočíselný, musí platit $det(A) = det(A^{-1}) = \pm 1$ neboť v okruhu $\mathbb{Z}$ máme pouze dvě jednotky a to právě ± 1.

Buď naopak $A \in Mat_{n\times m}\mathbb{Z}$ čtvercová s determinantem ± 1. Pak inverzní matici A^{-1} můžeme spočítat z algebraických doplňků jako

$$A^{-1} = \frac{1}{det(A)} \cdot A_{adj} = \pm A_{adj}$$

nicméně prvky matice A_{adj} - algebraické doplňky - se vypočítají ze subdeterminantů (minorů) matice A a musí být proto celočíselné. Matice A^{-1} je tedy celočíselná. □

Z tohoto lemmatu tedy plyne, že pokud chceme celočíselnou matici B převést do SNF pomocí invertibilních matic, musíme tak činit pouze prostřednictvím matic majících determinant ± 1. Nyní tedy můžeme přikročit k důkazu samotné věty o SNF .

Důkaz. (Věty o Smithově normálním tvaru). Nejprve dokážeme existenci SNF . Pro tento účel budeme potřebovat Euklidův algoritmus. Ten funguje následujícím způsobem.

Pro libovolná $a, b \in \mathbb{Z}$ taková, že $|a| > |b|$ vydělíme číslo a číslem b se zbytkem. Tedy $a = qb + c$. Pak ovšem platí, že $gcd(a,b) = gcd(b,c)$ neboť

$$gcd(a,b) = d \Rightarrow d|(a - qb) \Rightarrow d|c \Rightarrow d|gcd(b,c)$$

a naopak

$$gcd(b,c) = e \Rightarrow e|(qb + c) \Rightarrow e|a \Rightarrow e|gcd(a,b).$$

Takto můžeme postupovat rekurzivně a po konečném počtu kroků bude $c = 0$ a b příslušné danému kroku bude právě hledaný největší společný dělitel. Poznamenejme, že užití Euklidova algoritmu je z výpočetního hlediska výhodně, neboť má logaritmickou složitost.

Dále protože výsledné transformační matice P, Q musí být invertibilní nad $\mathbb{Z}$, plyne z předchozího lemmatu, že jejich determinant musí být roven ± 1. Evidentně tedy nemůžeme násobit řádek či sloupec matice jiným číslem než ± 1. Můžeme však prohodit libovolné dva řádky, protože to lze realizovat pomocí transformační matice,

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

která má evidentně determinant roven -1. Analogicky můžeme prohazovat prohazovat libovolné dva sloupce. A konečně pomocí transformační matice

$$\begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & \vdots & \ddots & & & \\ & & m & & 1 & & \\ & & & \dots & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

můžeme k libovolnému řádku přičíst m-násobek jiného řádku.

Nyní budeme postupovat následujícím způsobem. Na pozici $(1,1)$ přesuneme libovolný nenulový prvek matice B (Pokud $B = 0$, pak je již ve SNF a žádné operace provádět nemusíme). Pak postupně pro každý prvek pod a napravo od prvku b_1^1 aplikujeme Euklidův algoritmus (konkrétně jeho implementaci pomocí řádkových a sloupcových operací, která potřebuje pouze operace násobení řádku/sloupce číslem -1, přičítání násobku řádku/sloupce k jinému a prohazování dvou řádků/sloupců), čímž na pozici $(1,1)$ vyrobíme největší společný prvků v prvním sloupci a řádku. Tyto prvky můžeme tedy snadno vyeliminovat, čímž získáme matici ve tvaru

$$B = \begin{pmatrix} b_1^1 & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \dots & * \end{pmatrix}.$$

Pokud nyní existuje nějaký prvek b_j^i, který ještě není dělitelný b_1^1, můžeme přičíst j-tý sloupec k prvnímu sloupci a opět vyrobit na pozici $(1,1)$ prvek b'^1_1 takový, že $b'^1_1 | b_1^1$ a zároveň $b'^1_1 | b_j^i$, který jej již dělit bude. Poznamenejme, že tento prvek bude nutně menší než původní b_1^1, díky čemuž náš algoritmus skončí po konečném počtu kroků.

Celkem máme algoritmus, který převede matici B do výše uvedeného tvaru a navíc $b_1^1 | b_j^i$. Označme takto vzniklou matici C a nechť $q_k = c_1^1$. Nyní můžeme postupovat indukcí a aplikovat tento algoritmus na submatici, která vznikne vynecháním prvního sloupce a řádku matice C. Neboť q_k dělil všechny prvky matice C, bude dělit i prvek v levém horním rohu submatice (označme jej q_{k+1}) po aplikaci výše uvedeného algoritmu. Dostáváme, že $q_k | q_{k+1}$, což jsme měli dokázat.

Zbývá dokázat jednoznačnost. Označme

$$gcd_{i\times i}(A) = gcd\{det(X) | X \text{ je submatice } A \text{ tvaru } i \times i\}$$

Prvně ukážeme, že platí rovnost

$$q_1 \dots q_i = gcd_{i\times i}(A)$$

kde A je matice ve SNF . Pokud submatice X obsahuje k-tý řádek, ale neobsahuje k-tý sloupec matice A, bude její determinant evidentně nulový, neboť A je diagonální a X tak bude obsahovat nulový řádek. Stačí tedy uvažovat submatice jejichž diagonála leží na hlavní diagonále matice A. To znamená, že platí

$$gcd_{i\times i}(A) = gcd\{q_{k_1} \dots q_{k_i} | 1 \le k_1 < \dots < k_i \le r\}.$$

Navíc A je ve SNF , proto $q_i|q_{i+1}$ z čehož plyne

$$gcd\{q_{k_1}\dots q_{k_i}|1 \leq k_1 < \dots < k_i \leq r\} = q_1\dots q_i,$$

což jsme chtěli dokázat.

Konečně ukážeme, že největší společný dělitel subdeterminantů je invariantní vzhledem k elementárním řádkovým operacím (invariance vzhledem k sloupcovým operacím pak plyne ze symetrie).

Invariance vzhledem k násobení řádku číslem -1 a vzhledem k prohození řádků je zřejmá, neboť tyto operace maximálně změní znaménko některých subdeterminantů. To ovšem nemá žádný vliv na výsledného největšího společného dělitele. Pro přičítání násobku řádku je situace ovšem poněkud složitější. Každý nový subdeterminant je pak celočíselnou kombinací subdeterminantů předchozí matice. Z toho plyne, že

$$gcd_{i\times i}(A)|gcd_{i\times i}(A').$$

Jak jsme ale ukázali dříve, operace přičtení řádku je invertibilní. Můžeme tedy celý proces zopakovat opačným směrem a stejnou argumentací dostáváme

$$gcd_{i\times i}(A')|gcd_{i\times i}(A).$$

Největší společný dělitel subdeterminantů se tedy nezmění.

Předpokládejme nyní, že SNF není jednoznačný a existují matice A,C a P,Q,T,U takové, že platí $B = P\cdot A\cdot Q = T\cdot C\cdot U$, kde A,C jsou různé a ve SNF a P,Q,T,U jsou celočíselné invertibilní matice. Pak násobení invertibilními maticemi P,Q,T,U odpovídá postupnému provádění elemntárních řádkových a sloupcových úprav, o kterých jsme ovšem dokázali, že nemění největšího společného dělitele subdeterminantů. To speciálně znamená, že hlavní minory matic A,C ve Smithově normálním tvaru jsou si rovny a proto i invariatní faktory musí být stejně. To je spor s předpokladem. Smithův normální tvar je tedy jednoznačný.

□

1.1 Podkapitola

1.1.1 Odstavec

Kapitola 2

Triangularizace celočíselných matic

V této kapitole se budeme zabývat popisem algoritmu pro výpočet redukovaného schodovitého tvaru celočíselných matic. Tento algoritmus představil Arne Storjohann v článku nazvaném „*A fast+practial+deterministic algorithm for triangularizing integer matrices*" [6]. Definujme nejdříve tvar matice, jehož vytvoření bude našim cílem.

Definice 2.1. Řekneme že matice $A \in Mat_{n\times m}\mathbb{Z}$ je v redukovaném schodovitém tvaru (RST) jestliže splňuje následující podmínky:

(c1) Buď r hodnost matice A. Pak prvních r řádků je nenulových.

(c2) Pro každé $1 \leq i \leq r$ buď $A[i, j_i]$ první nenulový prvek v i-tém řádku. Pak $j_1 < j_2 < \cdots < j_r$.

(c3) Pro každé $1 \leq i \leq r$ platí $A[i, j_i] > 0$.

(c4) Pro každé $1 \leq k < i \leq r$ platí $A[i, j_i] > A[k, j_i] \geq 0$.

Poznámka 2.2. Poznamenejme, že první a druhá podmínka nám zaručují schodovitý tvar matice A. Tento však zjevně není jednoznačný. Proto je nutné přidat ještě podmínky (*c3*) a (*c4*). (*c3*) zajišťuje, že členy nad pivoty budou kladné a (*c4*) říká, že prvky nad pivoty budou pivoty omezeny. Tyto podmínky pak určují tvar matice A jednoznačně vzhledem k elementárním operacím.

Příklad 2.3. Pro ilustraci uvádíme následující matici v RST :

$$\begin{pmatrix} 2 & 33 & 6 & 0 & 39 & 73 \\ 0 & 0 & 24 & 0 & 444 & 8 \\ 0 & 0 & 0 & 1 & 22 & 23 \\ 0 & 0 & 0 & 0 & 0 & 75 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

V následujících podkapitolách nejdříve popíšeme několik klíčových procedur, které budou upravovat vstupní matici A, pomocí unimodulárních (mající determinant roven ± 1, tedy invertibilních) matic. Tyto procedury postupně propojíme a v poslední podkapitole pak obdržíme samotný algoritmus pro výpočet RST .

2.1 GCD redukce

Jak jsme viděli již v důkazu věty o Smithově normálním tvaru, častou operací, kterou s maticí při převodu do SNF provádíme, je eliminace všech prvků nacházejících se pod nějakým námi zvoleným pivotem. Takováto eliminace je poměrně náročná, neboť pro každý prvek musíme vytvářet největší společný dělitel s pivotem. Bylo by proto výhodné, kdybychom mohli nějakým způsobem upravit prvky ve sloupci tak, že největší společný dělitel nějakých dvou prvků daného sloupce bude zároveň největším společným dělitelem všech prvků daného sloupce. A přesně to je obsahem následující věty.

Věta 2.4 (GCD redukce)**.** *Nechť $B \in Mat_{n\times m}\mathbb{Z}$ je matice $(k+2)\times k$ a $rank(B) = 2$, kterou můžeme zapsat jako*

$$B = \begin{pmatrix} N & \bar{N} \\ a_0 & \bar{a}_0 \\ b_1 & \bar{b}_1 \\ \vdots & \vdots \\ b_k & \bar{b}_k \end{pmatrix},$$

kde N je kladné. Pak existuje deterministický algoritmus, který pro matici B vypočte unimodulární matici

$$C = \begin{pmatrix} 1 & & & & \\ & 1 & c_1 & \cdots & c_k \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

takovou, že bude platit

$$CB = \begin{pmatrix} N & \bar{N} \\ a_k & \bar{a}_k \\ b_1 & \bar{b}_1 \\ \vdots & \vdots \\ b_k & \bar{b}_k \end{pmatrix} \text{ kde dgsdgddg sdgsdgsdgdgsdgdsdg}$$

a navíc CB bude splňovat následující podmínky:

(c1) *hlavní submatice $\begin{pmatrix} N & \bar{N} \\ a_k & \bar{a}_k \end{pmatrix}$ je regulární a*

(c2) $gcd(N, a_k) = gcd(N, a_0, b_1, b_2, \ldots, b_k)$.

Důkaz. Bez újmy na obecnosti můžeme předpokládat, že $k > 0$. Pokud by k bylo nulové, můžeme zřejmě za C zvolit identitu, které splní naše požadavky. Dále můžeme předpokládat, že hlavní submatice je regulární a tedy platí $N\bar{a}_0 - \bar{N}a_0 \neq 0$. Pokud by tomu tak nebylo, přičteme k druhému řádku nějaký řádek $2 < s \leq k+2$, pro který platí $N\bar{b}_s - \bar{N}b_s \neq 0$. Takový řádek jistě bude existovat, neboť matice B má plnou hodnost. Výsledná matice pak

bude mít hlavní submatici regulární. Pro takto upravenou matici můžeme spočítat hledané koeficienty c_i a konečně ke koeficientu c_s přičteme 1, což bude přesně odpovídat onomu přičtení s-tého řádku, které jsme provedli na začátku.

Nyní ukážeme, jak iterativně vypočítat c_l pro $l = 1,\ldots,k$. Označme mezivýsledky našeho výpočtu následujícím způsobem:

$$\begin{aligned} a_l &= a_0 + c_1 b_1 + \cdots + c_l b_l \\ \bar{a}_l &= \bar{a}_0 + c_1 \bar{b}_1 + \cdots + c_l \bar{b}_l \end{aligned} \tag{2.1}$$

Po provedení kroku $l-1$ a na začátku kroku l jsou vypočítány koeficienty $c_1,\ldots,c_{l-1}$ a jsou splněny podmínky

(1) $gcd(N,a_i) = gcd(N,a_0,b_1,b_2,\ldots,b_i)$

(2) $N\bar{a}_i - \bar{N}a_i \neq 0$

pro $i = l-1$. Poznamenejme, že pro $i = 0$ jsou podmínky (1) a (2) splněny triviálně. Teď musíme provést indukční krok - najít vhodné c_l takové, že budou splněny podmínky (1) a (2) pro $i = l$.

Nechť $g = gcd(a_{l-1},b_l)$. Pak můžeme dělením se zbytkem najít celá čísla q_1,q_2 a $0 \leq \tilde{a}_{l-1},\tilde{b}_l < N$ taková, že platí

$$\begin{aligned} a_{l-1}/g &= q_1 N + \tilde{a}_{l-1} \\ b_l/g &= q_2 N + \tilde{b}_l \end{aligned} \tag{2.2}$$

Čísla $\tilde{a}_{l-1}$ a $\tilde{b}_l$ jsou nesoudělná, protože TODO. Pomocí algoritmu uvedeného v TODO můžeme najít nejmenší kladné číslo t takové, že bude platit

$$gcd(\tilde{a}_{l-1} + t\tilde{b}_l, N) = 1 \tag{2.3}$$

a volbou $c_l \leftarrow t$ zajistíme splnění podmínky (1). Skutečně:

$$\begin{aligned} gcd(a_l,N) &= gcd(a_{l-1} + tb_l, N) && \text{we are trying to solve for} \\ &= gcd(g(q_1N + \tilde{a}_{l-1}) + tg(q_2N + \tilde{b}_l), N) \\ &= gcd(g(\tilde{a}_{l-1} + t\tilde{b}_l) + g(q_1 + tq_2)N, N) \\ &= gcd(g(\tilde{a}_{l-1} + t\tilde{b}_l), N) \\ &= gcd(g, N) \\ &= gcd(a_{l-1}, b_l, N) \\ &= gcd(N, a_0, b_1, b_2, \ldots, b_l) \end{aligned}$$

přičemž poslední rovnost plyne z indukčního předpokladu.

Nakonec musíme zajistit splnění i druhé podmínky (2). Buď l index aktuálního kroku a předpokládejme, že platí

$$\begin{vmatrix} N & \bar{N} \\ a_{l-1} + xb_l & \bar{a}_{l-1} + x\bar{b}_l \end{vmatrix} = 0 \tag{2.4}$$

pak ovšem z indukčního předpokladu plyne, že $N\bar{b}_l - \bar{N}b_l \neq 0$. To implikuje, že prvek x je určen jednoznačně a můžeme jej vyjádřit jako

$$x = -\frac{N\bar{a}_{l-1} - \bar{N}a_{l-1}}{N\bar{b}_l - \bar{N}b_l} \tag{2.5}$$

Pokud bychom v kroku 2.3 □

2.2 Podkapitola

Závěr

Příloha

Sem můžete přidat přílohu. Pokud chcete "přílohy", tak upravte definici záhlaví v souboru sci.muni.thesis.sty, viz řádek 644.

Seznam použité literatury

[1] S. J. Monaquel a K. M. Schmidt, *On M-functions and operator theory for non-self-adjoint discrete Hamiltonian systems*, v „Special Issue: 65th birthday of Prof. Desmond Evans“, J.Comput. Appl. Math. **208** (2007), č. 1, 82–101.

[2] M. Murata, *Positive solutions and large time behaviors of Schrödinger semigroups, Simon's problem*, J. Funct. Anal. **56** (1984), č. 3, 300–310.

[3] J. Qi a S. Chen, *Strong limit-point classification of singular Hamiltonian expressions*, Proc. Amer. Math. Soc. **132** (2004), č. 6, 1667–1674 (elektronicky).

[4] Z. Pospíšil, *An inverse problem for matrix trigonometric and hyperbolic functions on measure chains*, v „Colloquium on Differential and Difference Equations — CDDE 2002“ (Brno, 2002), Folia Fac. Sci. Natur. Univ. Masaryk. Brun. Math. **13**, str. 205–211, Masarykova univerzita, Brno, 2003.

[5] R. Šimon Hilscher a P. Zemánek, *Friedrichs extension of operators defined by linear Hamiltonian systems on unbounded interval*, v „Equadiff 12“, Proceedings of the Conference on Differential Equations and their Applications (Brno, 2009), J. Diblík, O. Došlý, P. Drábek a E. Feistauer, editoři, Math. Bohem. **135** (2010), č. 2, 209–222.

[6] A. Storjohann, *A Fast+Practical+Deterministic Algorithm for Triangularizing Integer Matrices*, Cosi, Springer-Verlag, Zurich, 1996.