STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor: 1. Matematika a statistika

Mřížová kryptografie nad duálními čísly

Dominik Doležel

Brno 2024

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

MŘÍŽOVÁ KRYPTOGRAFIE NAD DUÁLNÍMI ČÍSLY

LATTICE CRYPTOGRAPHY OVER DUAL INTEGERS

AUTOR	Dominik Doležel
ŠKOLA	Gymnázium Brno, třída Kpt. Jaroše
KRAJ	Jihomoravský
ŠKOLITEL	doc. RNDr. Miroslav Kureš, Ph.D.
OBOR	1. Matematika a statistika

Brno 2024

Prohlášení

Prohlašuji, že svou práci na téma *Mřížová kryptografie nad duálními čísly* jsem vypracoval/a samostatně pod vedením doc. RNDr. Miroslava Kureše, Ph.D. a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Dále prohlašuji, že tištěná i elektronická verze práce SOČ jsou shodné a nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon) v platném znění.

V Brně dne: _____

_____

Dominik Doležel

Poděkování

Především děkuji mé spolužačce Hance Trubačíkové, jež mi našla toho nejlepšího školitele, kterého jsem si mohl přát.

Tato práce byla provedena za finanční podpory Jihomoravského kraje.

Anotace

Goldreich-Goldwasser-Halevi kryptosystém byl publikován v roce 1997 stejnojmennými autory. Jedná se o asymetrický kryptosystém se soukromým a veřejným klíčem. Jeho výhodou oproti ostatním kryptosystémům je to, že se prozatím považuje za kvantově neprolomitelný. Využívá tzv. „problému nejbližšího vektoru“ (z angl. *closest vector problem*), též CVP, tedy hledání nejbližší lineární kombinace vektorů base dané mříže.

Dva roky po jeho představení se zjistilo, že jenom pomocí veřejného klíče lze vyčíst informace o zprávě (Nguyenův útok). Pro matice větších řádů (cca stovek) je však v podstatě neškodný.

Cílem práce je ověřit, zda lze tento kryptosystém konstruovat i nad okruhem duálních celých čísel a zda případně zvyšují jeho bezpečnost vzhledem k Nguyenově útoku.

Klíčová slova

kryptografie, GGH, duální čísla, matice, mříž, vektor, kryptosystém s veřejným klíčem

Annotation

The Goldreich-Goldwasser-Halevi cryptosystem was first published in 1979. It is an assymetric cryptosystem with a private and a public key. Its advantage compared to other cryptosystems is the fact that it is thought to be quantum-safe, at least for now. It is based on the *closest vector problem* (or CVP for short), meaning the search of the closest linear combination of vectors of the basis of a given lattice.

Two years after its initial publication it was found out that it is possible

to get some information about the message just from looking at the public key (Nguyen attack). But it is basically useless for matrices of higher order (approx. hundreds).

We study if it is possible to construct this cryptosystem over the ring of dual integers and if so, wheter it improves its safety in any way.

Keywords

cryptography, GGH, dual numbers, matrix, lattice, vector, cryptosystem with public key

Obsah

Úvod

Pojem duálních čísel byl poprvé představen W. K. Cliffordem v roce 1873, jejich aplikace pak studoval o dvacet let později A. P. Kotelnikov. Jedná se o komutativní okruh s jedničkou, jak ukážeme v kapitole *Obecné poznatky*. V praxi se duální čísla používají pro automatickou diferenciaci či popisování rotace.

Pánové C. Towse a E. Campbell v jejich článku přišli s algoritmem, kterým konstruují celočíselné matice s celočíselnými vlastními hodnotami. To je užitečné především z didaktických důvodů: při představování nového konceptu studentům se hodí, aby byly výsledky celočíselné. V první části této práce prozkoumáme, zda lze tento algoritmus použít i nad duálními čísly, popřípadě jak ho upravit tak, aby použitelný byl.

V druhé části se pak zaměříme na kryptosystém GGH. Ten je sice kvantově neprolomitelný, ale není stoprocentně odolný vůči jiným hrozbám (jako třeba Nguyenův útok). Cílem této práce je zjistit, zda jej lze zkonstruovat nad duálními čísly a zda se tím případně zvyšuje jeho bezpečnost.

Dalším cílem je naprogramovat celý kryptosystém v jazyce C++.

Obecné poznatky

Zavedení duálních čísel

V této části zavedeme pojem *duálních čísel* tak, jak to v roce 1873 udělal W. K. Clifford a ukážeme, že spolu se sčítáním a násobením se jedná o komutativní okruh s jednotkovým prvkem.

Definice 1. Nechť je dán komutativní okruh R. Potom množinu

$$R[\varepsilon] = \left\{a + b\varepsilon; \varepsilon^2 = 0; a, b \in R\right\}$$

nazveme *duálním rozšířením* tohoto okruhu R. Taková čísla budeme obvykle značit $\boldsymbol{a} = a_0 + a_1\varepsilon$. Čísla a_0 (resp. $a_1\varepsilon$) nazýváme *regulární* (resp. *nilpotentní*) *částí* čísla $\boldsymbol{a}$. [**dual-numbers**]

Zvláště zajímavé jsou potom pro nás takto rozšířené komutativní okruhy reálných a celých čísel.

Definice 2. Množiny

- $\mathbb{R}[\varepsilon] = \mathbb{D} = \{a + b\varepsilon; \varepsilon^2 = 0; a, b \in \mathbb{R}\}$ nazveme *duálními čísly*,
- $\mathbb{Z}[\varepsilon] = \{a + b\varepsilon; \varepsilon^2 = 0; a, b \in \mathbb{Z}\}$ nazveme *duálními celými čísly*.

Na těchto množinách potom definujeme operace *sčítání* a *násobení*.

Definice 3. Nechť je dána množina $R[\varepsilon]$. Potom operace $+ : R[\varepsilon] \times R[\varepsilon] \to R[\varepsilon]$ (*sčítání*) a $\cdot : R[\varepsilon] \times R[\varepsilon] \to R[\varepsilon]$ (*násobení*) definujeme následovně:

$$\forall \boldsymbol{a}, \boldsymbol{b} \in R[\varepsilon] : \boldsymbol{a} + \boldsymbol{b} = (a_0 + a_1) + (b_0 + b_1) = (a_0 + b_0) + (a_1 + b_1)\varepsilon,$$

$$\forall \boldsymbol{a}, \boldsymbol{b} \in R[\varepsilon] : \boldsymbol{a} \cdot \boldsymbol{b} = (a_0 + a_1\varepsilon) \cdot (b_0 + b_1\varepsilon) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\varepsilon.$$

Pro zkrácení zápisu často vynecháváme znak „$\cdot$“ a píšeme jenom $\boldsymbol{ab}$.

Věta 1. Nechť je dán komutativní okruh s jedničkou R. Potom $R[\varepsilon]$ je taky komutativní okruh s jedničkou.

Důkaz. Předveďme obecný důkaz pro $R[\varepsilon]$, pro ostatní případy se postupuje obdobně.

(i) operace sčítání i násobení jsou podle definice 3 na dané množině uzavřené,

(ii) sčítání je asociativní, protože

$$\begin{aligned}\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in R[\varepsilon] : (\boldsymbol{a} + \boldsymbol{b}) + \boldsymbol{c} &= [(a_0 + b_0) + (a_1 + b_1)\varepsilon] + (c_0 + c_1\varepsilon) \\ &= (a_0 + b_0 + c_0) + (a_1 + b_1 + c_1)\varepsilon \\ &= (a_0 + a_1\varepsilon) + [(b_0 + c_0) + (b_1 + c_1)\varepsilon] \\ &= \boldsymbol{a} + (\boldsymbol{b} + \boldsymbol{c}),\end{aligned}$$

(iii) neutrální prvek vzhledem ke sčítání je $0 + 0\varepsilon$, protože

$$\forall \boldsymbol{a} \in R[\varepsilon] : (0 + 0\varepsilon) + (a_0 + a_1\varepsilon) = (a_0 + 0) + (a_1 + 0)\varepsilon = a_0 + a_1\varepsilon,$$

(iv) opačný prvek k $\boldsymbol{a}$ vzhledem ke sčítání je $-\boldsymbol{a}$, protože

$$\begin{aligned}&\forall \boldsymbol{a} \in R[\varepsilon] : \boldsymbol{a} + (-\boldsymbol{a}) = \\ &= (a_0 + a_1\varepsilon) - (a_0 + a_1\varepsilon) \\ &= (a_0 - a_0) + (a_1 - a_1)\varepsilon = 0 + 0\varepsilon,\end{aligned}$$

(v) sčítání je komutativní, protože

$$\begin{aligned}\forall \boldsymbol{a}, \boldsymbol{b} \in R[\varepsilon] : \boldsymbol{a} + \boldsymbol{b} &= (a_0 + a_1\varepsilon) + (b_0 + b_1\varepsilon) \\ &= (a_0 + b_0) + (a_1 + b_1)\varepsilon \\ &= (b_0 + b_1\varepsilon) + (a_0 + a_1\varepsilon) = \boldsymbol{b} + \boldsymbol{a},\end{aligned}$$

(*vi*) násobení je asociativní, protože

$$\begin{aligned}\forall \boldsymbol{a},\boldsymbol{b},\boldsymbol{c} \in R[\varepsilon] : (\boldsymbol{ab})\boldsymbol{c} &= [(a_0+a_1\varepsilon)(b_0+b_1\varepsilon)]\,(c_0+c_1\varepsilon)\\ &= [a_0b_0+(a_0b_1+a_1b_0)\varepsilon]\,(c_0+c_1\varepsilon)\\ &= a_0b_0c_0+(a_1b_0c_0+a_0b_1c_0+a_0b_0c_1)\varepsilon\\ &= (a_0+a_1\varepsilon)\,[b_0c_0+(b_0c_1+b_1c_0)\varepsilon]\\ &= (a_0+a_1\varepsilon)\,[(b_0+b_1\varepsilon)(c_0+c_1\varepsilon)] = \boldsymbol{a}(\boldsymbol{bc}),\end{aligned}$$

(*vii*) jednotkový prvek (vzhledem k násobení) je $1+0\varepsilon$, protože

$$\begin{aligned}\forall \boldsymbol{a} \in R[\varepsilon] : \boldsymbol{a}(1+0\varepsilon) &= (a_0+a_1\varepsilon)(1+0\varepsilon)\\ &= a_0+(0\cdot a_0+1\cdot a_1)\varepsilon\\ &= a_0+a_1\varepsilon = \boldsymbol{a},\end{aligned}$$

(*viii*) sčítání je „k násobení“ distributivní, protože

$$\begin{aligned}&\forall \boldsymbol{a},\boldsymbol{b},\boldsymbol{c} \in R[\varepsilon] : \boldsymbol{a}(\boldsymbol{b}+\boldsymbol{c}) =\\ &= (a_0+a_1\varepsilon)\,[(b_0+b_1\varepsilon)+(c_0+c_1\varepsilon)]\\ &= (a_0+a_1\varepsilon)\,[(b_0+c_0)+(b_1+c_1)\varepsilon]\\ &= a_0(b_0+c_0)+[a_0(b_1+c_1)+a_1(b_0+c_0)]\,\varepsilon\\ &= (a_0b_0+a_0c_0)+(a_0b_1+a_0c_1+a_1b_0+a_1c_0)\varepsilon\\ &= [a_0b_0+(a_0b_1+a_1b_0)\varepsilon]+[a_0c_0+(a_0c_1+a_1c_0)\varepsilon]\\ &= (a_0+a_1\varepsilon)(b_0+b_1\varepsilon)+(a_0+a_1\varepsilon)(c_0+c_1\varepsilon) = \boldsymbol{ab}+\boldsymbol{ac},\end{aligned}$$

(ix) násobení je „ke sčítání“ distributivní, protože

$$\begin{aligned}
&\forall \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in R[\varepsilon] : (\boldsymbol{a}+\boldsymbol{b})\boldsymbol{c} = \\
&= [(a_0 + a_1\varepsilon) + (b_0 + b_1\varepsilon)]\,(c_0 + c_1\varepsilon) \\
&= [(a_0 + b_0) + (a_1 + b_1)\varepsilon]\,(c_0 + c_1\varepsilon) \\
&= (a_0 + b_0)c_0 + [(a_1 + b_1)c_0 + (a_0 + b_0)c_1]\,\varepsilon \\
&= a_0c_0 + b_0c_0 + (a_1c_0 + b_1c_0 + a_0c_1 + b_0c_1)\varepsilon \\
&= [a_0c_0 + (a_0c_1 + a_1c_0)\varepsilon] + [b_0c_0 + (b_0c_1 + b_1c_0)\varepsilon] \\
&= (a_0 + a_1\varepsilon)(c_0 + c_1\varepsilon) + (b_0 + b_1\varepsilon)(c_0 + c_1\varepsilon) = \boldsymbol{a}\boldsymbol{c} + \boldsymbol{b}\boldsymbol{c},
\end{aligned}$$

takže opravdu, $R[\varepsilon]$ je komutativní okruh s jedničkou. □

Zejména $\mathbb{Z}[\varepsilon]$ a $\mathbb{R}[\varepsilon]$ jsou komutativní okruhy s jedničkou. $R[\varepsilon]$ však není oborem integrity. Například v $\mathbb{Z}[\varepsilon]$ platí:

$$\forall \boldsymbol{k}, \boldsymbol{l} \in \mathbb{Z}[\varepsilon], k_0 = l_0 = 0 : k_1\varepsilon \cdot l_1\varepsilon = 0,$$

tedy součin dvou nenulových prvků může býti nulovým prvkem.

Poznámka. Ne všechny nenulové prvky $R[\varepsilon]$ mají inversní prvek vzhledem k násobení. Hledejme inversi $\boldsymbol{b}$ k $\boldsymbol{a}$. Platí

$$\begin{aligned}
1 + 0\varepsilon &= (a_0 + a_1\varepsilon)(b_0 + b_1\varepsilon) \\
&= a_0b_0 + a_0b_1\varepsilon + a_1b_0\varepsilon \implies a_0b_0 = 1 \iff b_0 = \frac{1}{a_0} \\
&\text{a } b_1 = -\frac{a_1b_0}{a_0} = -\frac{a_1}{a_0^2},
\end{aligned}$$

odkud vidíme, že nejen neutrální prvek vzhledem ke sčítání, ale ani žádný prvek tvaru $0 + k\varepsilon$, $k \in R$, není invertibilní. Proto taky duální čísla nejsou tělesem.

Vlastnosti duálních čísel

V této části se zaměříme na další operace s duálními čísly. Představíme problémy s dělením, dále zavedeme dělitelnost, kongruenci a odmocninu.

Definice 4. *Dělením* v R se rozumí taková binární operace $\varphi : R \times R \to R$, jež každé uspořádané dvojici (jednotlivým prvkům říkáme *dělenec* a *dělitel*) přiřadí jednoznačný obraz (tomu říkáme *podíl*), přičemž platí

$$\varphi(a, b) = c, \text{ kde } a = bc, b \neq 0.$$

Zkráceně pak píšeme $a : b = c$.

Věta 2. $\forall a, b \in \mathbb{R} - \{0\} : ab \neq 0$.

Důkaz. Předpokládejme, že existují dvě nenulová $a, b \in \mathbb{R}$ taková, že platí $ab = 0$. Potom, protože b je nenulové, můžeme jím rovnici vydělit. Dostáváme tedy

$$a = \frac{0}{b} = 0,$$

což je spor s předpokladem, že a je nenulové. □

Poznámka. Protože $\mathbb{Z}[\varepsilon]$ není oborem integrity, může být dělení nedefinováno, i když je dělitel nenulový. To je vidět v následujícím příkladu.

Příklad 1. Kolik je $6\varepsilon : 3\varepsilon$? Výsledků je nekonečně mnoho. Všechny jsou tvaru $2 + k\varepsilon$, kde $k \in \mathbb{R}$. Proto se nejedná o zobrazení – jeden vzor má více obrazů.

Pokud je regulární část čísel nenulová, postupujeme „usměrňovacím“ způsobem, jak je vidět v následujícím příkladu.

Příklad 2. Spočtěte $(6 + 5\varepsilon) : (2 + 3\varepsilon)$.

$$\frac{6 + 5\varepsilon}{2 + 3\varepsilon} = \frac{6 + 5\varepsilon}{2 + 3\varepsilon} \cdot \frac{2 - 3\varepsilon}{2 - 3\varepsilon} = \frac{(6 + 5\varepsilon)(2 - 3\varepsilon)}{2^2 - (3\varepsilon)^2} = \frac{12 - 8\varepsilon}{4} = 3 - 2\varepsilon$$

Definice 5. Nechť $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Z}[\varepsilon]$. Řekneme, že $\boldsymbol{a}$ *dělí* $\boldsymbol{b}$, jestliže existuje takové $\boldsymbol{c}$, že $\boldsymbol{ac} = \boldsymbol{b}$.

Věta 3. Nechť jsou $\boldsymbol{a} = a_0 + a_1\varepsilon$, $\boldsymbol{b} = b_0 + b_1\varepsilon \in \mathbb{Z}[\varepsilon]$. Potom

(*i*) $\boldsymbol{b}$ je *regulárním dělitelem* $\boldsymbol{a}$ právě tehdy, když $0 \neq b_0 \,|\, a_0 \wedge b_0^2 \,|\, (a_0b_1 - a_1b_0)$;

(*ii*) $\boldsymbol{b}$ je *nilpotentním dělitelem* $\boldsymbol{a}$ právě tehdy, když $a_0 = b_0 = 0 \wedge b_1 \,|\, a_1$;

(*iii*) ve všech ostatních případech $\boldsymbol{b}$ není dělitelem $\boldsymbol{a}$.

Důkaz. (*i*) Začněme zjednodušením výrazu

$$\frac{a_0 + a_1\varepsilon}{b_0 + b_1\varepsilon} \cdot \frac{b_0 - b_1\varepsilon}{b_0 - b_1\varepsilon} = \frac{a_0b_0 + (a_0b_1 + a_1b_0)\varepsilon}{b_0^2},$$

což je duální celé číslo právě tehdy, když jeho regulární a nilpotentní část jsou celá čísla, tedy $b_0^2 \,|\, a_0b_0 \iff b_0 \,|\, a_0$ a $b_0^2 \,|\, (a_0b_1 + a_1b_0)$, což jsme chtěli dokázat.

(*ii*) Duální celé číslo tvaru $b_1\varepsilon$ dělí $a_1\varepsilon$ triviálně právě tehdy, když $b_1 \,|\, a_1$.

(*iii*) Zbývající možnost, jež není obsažena v bodech (*i*) a (*ii*) je $b_0 = 0 \wedge a_0 \neq 0$. Ale potom $\boldsymbol{b}$ nemůže dělit $\boldsymbol{a}$, protože $\boldsymbol{b} \cdot \boldsymbol{k}, \boldsymbol{k} \in \mathbb{Z}[\varepsilon]$ se nemůže rovnat $\boldsymbol{a}$, protože $a_0 \neq 0$. □

V $\mathbb{Z}$ je klasicky definován *největší společný dělitel* d čísel a, b. Stojí za to si povšimnout, že pokud $a, b \neq 0$, jsou největší společní dělitelé ke každé takové dvojici právě dva, přičemž $d_1 = -d_2$. [**delitelnost**]

Definice 6. *Největší společný dělitel* čísel $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}[\varepsilon]$ je takové číslo $\boldsymbol{d} \in \mathbb{Z}[\varepsilon]$, pro něž platí, že dělitel:

- je společný, to jest $\boldsymbol{d} \,|\, \boldsymbol{a} \wedge \boldsymbol{d} \,|\, \boldsymbol{b}$,
- je největší, to jest pro všechny ostatní společné dělitele $\boldsymbol{a}, \boldsymbol{b}$ platí, že dělí $\boldsymbol{d}$.

Často zapisujeme $\boldsymbol{d} = \gcd(\boldsymbol{a}, \boldsymbol{b})$.

V $\mathbb{Z}[\varepsilon]$ nemusí být největší společný dělitel dvou čísel vždy definován. Vezměme $\boldsymbol{a} = \varepsilon$, $\boldsymbol{b} = 2\varepsilon$. Potom $1 + \varepsilon$ je jejich společný dělitel, protože po vynásobení ε dostáváme ε a po vynásobení 2ε dostáváme 2ε. Obdobně je společný dělitel i $1 + 2\varepsilon$, $1 + 3\varepsilon$ a vlastně všechna čísla tvaru $\pm 1 + k\varepsilon$, kde $k \in \mathbb{Z}$. Největší ze společných dělitelů ale není žádný – postupujme matematickou indukcí. Předpokládejme, že největší společný dělitel je ε. 2ε je společný dělitel obou těchto čísel, 4ε také, ..., navíc každý z nich dělí ten předchozí, takže největší společný dělitel neexistuje, protože vždy lze najít „většího“.

Definice 7. Nechť $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Z}[\varepsilon], \boldsymbol{c} \neq 0$. Potom řekneme, že $\boldsymbol{a}$ *je kongruentní* s $\boldsymbol{b}$ *modulo* $\boldsymbol{c}$ právě tehdy, když $\boldsymbol{c} \mid (\boldsymbol{a} - \boldsymbol{b})$. Píšeme $\boldsymbol{a} \equiv \boldsymbol{b} \mod \boldsymbol{c}$.

Uveďme skutečnost, již budeme později potřebovat.

Lemma 1. Nechť $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}[\varepsilon], \boldsymbol{a} \neq \boldsymbol{b}$. Potom

$$\boldsymbol{x} \equiv \boldsymbol{y} \mod \boldsymbol{a} - \boldsymbol{b} \implies \boldsymbol{ax} - \boldsymbol{by} \equiv 0 \mod \boldsymbol{a} - \boldsymbol{b}.$$

Důkaz. $\boldsymbol{x} \equiv \boldsymbol{y} \mod \boldsymbol{a} - \boldsymbol{b}$ lze přepsat jako $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{c}(\boldsymbol{a} - \boldsymbol{b})$ pro nějaké $\boldsymbol{c} \in \mathbb{Z}[\varepsilon]$. Potom $\boldsymbol{ax} - \boldsymbol{by} = \boldsymbol{ax} - \boldsymbol{b}\,[\boldsymbol{x} + \boldsymbol{c}(\boldsymbol{a} - \boldsymbol{b})] = (\boldsymbol{a} - \boldsymbol{b})(\boldsymbol{x} - \boldsymbol{bc})$. □

Dále lze obdobně jako v reálných číslech definovat odmocninu.

Definice 8. *Odmocninou* čísla $\boldsymbol{a} \in \mathbb{R}_0^+[\varepsilon]$ nazveme takové číslo $\boldsymbol{b} \in \mathbb{R}_0^+[\varepsilon]$, pro něž platí $\boldsymbol{b}^2 = \boldsymbol{a}$.

Věta 4. Nechť je dáno $\boldsymbol{a} \in \mathbb{R}_0^+[\varepsilon]$. Potom

$$\sqrt{\boldsymbol{a}} = \sqrt{a_0} + \frac{a_1}{2\sqrt{a_0}}\varepsilon.$$

Důkaz. Z definice plyne $\boldsymbol{a} = (b_0 + b_1\varepsilon)^2 = b_0^2 + 2b_0b_1 + (b_1\varepsilon)^2 = b_0^2 + 2b_0b_1$ pro nějaké $\boldsymbol{b} \in \mathbb{R}_0^+[\varepsilon]$, odkud získáváme $a_0 = b_0^2$, $b_1 = \frac{a_1}{2b_0} = \frac{a_1}{2\sqrt{a_0}}$. □

Poznámka.

- Uvědomme si, že má-li být odmocnina z $\boldsymbol{a}$ definována, musí být definována odmocnina z a_0, tedy $a_0 > 0$.
- Odmocnina z $\boldsymbol{a}$ je celé číslo právě tehdy, když $\sqrt{a_0} \in \mathbb{Z} \wedge 2\sqrt{a_0} \mid a_1$.

V této kapitole jsme zavedli pojem duálních čísel. Dokázali jsme, že se jedná o komutativní okruh s jedničkou.

Dále jsme zavedli pojmy dělitelnosti, kongruence a operace odmocniny.

Základní pojmy z lineární algebry

Pro pochopení následujících kapitol je nutné zavést určité pojmy.

Připomeňme čtenáři, co jsou to matice. Lze je definovat obecněji, pro naše účely se však omezíme na ty nad algebraickými okruhy. Nechť A je okruh s operacemi *sčítání* a *násobení* a k, l přirozená čísla. *Maticí typu* $k \times l$ *nad množinou* M budeme rozumět obdélníkové schéma

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{21} & a_{22} & \dots & a_{2l} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kl} \end{pmatrix},$$

kde $a_{ij} \in A$ pro každé $i = 1, \dots, k$ a $j = 1, \dots, l$. Jestliže $k = l$, hovoříme o *čtvercové matici řádu* k, v opačném případě o *obdélníkové matici typu* $k \times l$. Dále říkáme, že prvek a_{ij} stojí v matici na místě ij. [**lingebra**]

Nechť je dána množina všech matic M. Pak na množině M definujeme následující operace:

- sčítání matic ($M \times M \to M$) a násobení matice skalárem ($\mathbb{R} \times M \to M$): po složkách,
- násobení matic ($M \times M \to M$),
- adjugovaná ($M \to M$), inversní ($M \to M$), transponovaná matice ($M \to M$),

- determinant ($M \to \mathbb{R}$).

Předkládání podrobných definic uvedených pojmů však není předmětem této práce.

Definice 9. Čtvercová matice A je

- *singulární* právě tehdy, když nemá multiplikativní inversi,
- *unimodulární* právě tehdy, když všechny její prvky jsou ze $\mathbb{Z}$ a má multiplikativní inversi takovou, že všechny její prvky jsou ze $\mathbb{Z}$ a $AA^{-1} = A^{-1}A = I$.

Důsledek 1. (*i*) Singulární matice mají $\det A = 0$,

(*ii*) unimodulární matice mají $\det A = \pm 1$,

(*iii*) pokud je A unimodulární, pak i A^{-1} je unimodulární,

(*iv*) pokud A a B jsou unimodulární, pak i AB je unimodulární.

Definice 10. Nechť je dán vektor $\vec{v} = (v_1, v_2, \ldots, v_k)$ a čtvercová matice A řádu $n \in \mathbb{N}$. Pokud je splněna následující rovnost

$$A \cdot \vec{v} = \lambda \cdot \vec{v},$$

je $\vec{v}$ *vlastním vektorem* matice A a λ *vlastní hodnotou* této matice.

Příklad 3. Hledejme vlastní hodnoty a vlastní vektory matice

$$A = \begin{pmatrix} -6 & 13 & -1 \\ -8 & 13 & 0 \\ -17 & 23 & 2 \end{pmatrix}.$$

Řešme rovnici

$$\begin{aligned} A\vec{v} &= \lambda\vec{v} \\ A\vec{v} - \lambda\vec{v} &= \vec{o} \\ (A - \lambda I)\vec{v} &= \vec{o}. \end{aligned}$$

Aby vyšel nulový vektor, musí jeden z členů mít nulový determinant, resp. být nulový. Vektor $\vec{v}$ nulový být nemůže, protože hledáme nenulová řešení, takže $\det(A - \lambda I) = 0$. Po vyřešení rovnice získáme

$$\lambda \in \{1, 3, 5\}.$$

Ještě zbývá určit vlastní vektory k jednotlivým vlastním hodnotám.

(*i*) $\lambda = 1$: řešíme rovnici

$$\begin{pmatrix} -7 & 13 & -1 \\ -8 & 12 & 0 \\ -17 & 23 & 1 \end{pmatrix} \cdot \vec{v} = \vec{o}$$

Dostáváme řešení $t \cdot \left(\frac{3}{5}, \frac{2}{5}, 1\right), t \in \mathbb{R}$. Vlastní vektory jsou tedy vektory prostoru generovaného vektorem $\left(\frac{3}{5}, \frac{2}{5}, 1\right)$.

(*ii*) $\lambda = 3$: obdobně vlastní vektory jsou všechny vektory prostoru $\left[\left(\frac{5}{7}, \frac{4}{7}, 1\right)\right]$.

(*iii*) $\lambda = 5$: obdobně vlastní vektory jsou všechny vektory prostoru $\left[\left(\frac{1}{2}, \frac{1}{2}, 1\right)\right]$.

Vlastní vektory jsou tedy vektory prostorů $\left[\left(\frac{3}{5}, \frac{2}{5}, 1\right)\right], \left[\left(\frac{5}{7}, \frac{4}{7}, 1\right)\right], \left[\left(\frac{1}{2}, \frac{1}{2}, 1\right)\right]$.

Zaměřme se na geometrický význam vlastních vektorů a vlastních čísel. Mějme v třídimensionálním prostoru nějaké těleso, třeba krychli. Pak jeho vrcholy lze representovat jako osm vektorů vycházejících z počátku do těchto bodů. Při vynásobení maticí se prostor různě smršťí, roztáhne a natočí tak, že těchto osm vrcholů už nemusí ani ohraničovat krychli. Z definitorického vztahu vlastních čísel a vlastních vektorů $A\vec{v} = \lambda\vec{v}$ vlastně vidíme, že řešením takové rovnice jsou ty vektory, které se po vynásobení maticí chovají stejně, jako kdyby byly vynásobeny skalárem. Z teorie o vektorových prostorech víme, že vynásobení vektoru $\vec{v}$ skalárem k znamená zvětšení (nebo zmenšení) tohoto vektoru s koeficientem k při zachování jeho směru. [**lingebra**] Jinými slovy; vlastní vektory jsou takové vektory, které při vynásobení touto maticí nemění směr a jejich velikost se zvětší (nebo zmenší) λ-krát.

Důsledek 2. Identická matice řádu n má vlastní vektory z celé roviny, prostoru atd. tvaru $(v_1, v_2 \ldots, v_n), v_i \in \mathbb{R}$.

Důkaz. Řešme rovnici

$$\begin{aligned} I\vec{v} &= \lambda\vec{v} \\ (I - \lambda I)\vec{v} &= \vec{o} \\ \begin{pmatrix} 1-\lambda & 0 & \ldots & 0 \\ 0 & 1-\lambda & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1-\lambda \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \end{aligned}$$

dostáváme tedy soustavu rovnic

$$\begin{aligned} (1-\lambda)v_1 &= 0, \\ (1-\lambda)v_2 &= 0, \\ &\vdots \\ (1-\lambda)v_n &= 0, \end{aligned}$$

takže řešením je $\lambda = 1$ a všechny vektory $(v_1, v_2, \ldots, v_n), v_i \in \mathbb{R}$. □

V této kapitole jsme uvedli některé pojmy, které budeme potřebovat pro pochopení následujících kapitol.

O Towse-Campbellově konstrukci

S určováním vlastních hodnot a vlastních vektorů matic jsou studenti universit běžně seznamováni. Při představování této problematiky je vhodné, když jsou příklady co nejjednodušší, aby se pro výpočty nemusela používat kalkulačka (či dokonce počítačové programy jako Wolfram Mathematica). Přitom celočíselných matic s celočíselnými vlastními hodnotami je málo. C. Towse a E. Campbell v jejich práci navrhli algoritmus, jímž lze právě takové matice konstruovat.

V celých číslech

Představme nyní, na co přišli Towse a Campbell v jejich článku.

Definice 11. O matici A řekneme, že je *IMIE* (*Integer Matrix with Integer Eigenvalues*), pokud všechny její prvky i všechny její vlastní hodnoty jsou celá čísla.

Věta 5. Nechť je dána regulární celočíselná matice P řádu n a diagonální celočíselná matice D téhož řádu, přičemž prvky na její hlavní diagonále jsou navzájem kongruentní modulo $\det P$. Potom matice $A = PDP^{-1}$ je *IMIE*, přičemž její vlastní hodnoty jsou prvky na diagonále D.

Důkaz tohoto tvrzení je k nalezení v Towse-Campbellově článku. [**towse-campbell**] My se nyní zaměříme na otázku, zda lze toto tvrzení formulovat v duálních číslech.

V duálních číslech

Definice 12. O matici $\boldsymbol{A}$ řekneme, že je *DIMDIE* (*Dual Integer Matrix with Dual Integer Eigenvalues*), pokud všechny její prvky i všechny její vlastní hodnoty jsou duální celá čísla.

Věta 6. Nechť je dána regulární matice $\boldsymbol{P}$ řádu n nad $\mathbb{Z}[\varepsilon]$ a diagonální matice $\boldsymbol{D}$ téhož řádu nad $\mathbb{Z}[\varepsilon]$ následovně:

$$\boldsymbol{P} = \begin{pmatrix} \mathbf{p}_{11} & \mathbf{p}_{12} & \dots & \mathbf{p}_{1n} \\ \mathbf{p}_{21} & \mathbf{p}_{22} & \dots & \mathbf{p}_{2n} \\ \vdots & \vdots & & \vdots \\ \mathbf{p}_{n1} & \mathbf{p}_{n2} & \dots & \mathbf{p}_{nn} \end{pmatrix}, \boldsymbol{D} = \begin{pmatrix} \boldsymbol{\lambda}_1 & 0 & \dots & 0 \\ 0 & \boldsymbol{\lambda}_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \boldsymbol{\lambda}_n \end{pmatrix},$$

přičemž $\boldsymbol{\lambda}_1 \equiv \boldsymbol{\lambda}_2 \equiv \cdots \equiv \boldsymbol{\lambda}_n \mod \det \boldsymbol{P}$. Potom matice $\boldsymbol{A} = \boldsymbol{P}\boldsymbol{D}\boldsymbol{P}^{-1}$ je *DIMDIE* s vlastními hodnotami $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \dots, \boldsymbol{\lambda}_n$.

Důkaz. Dokažme nejprve, že všechny prvky $\boldsymbol{A}$ jsou duálními celými čísly. Když $\boldsymbol{A} = \boldsymbol{P}\boldsymbol{D}\boldsymbol{P}^{-1} = \frac{\boldsymbol{P}\boldsymbol{D}\operatorname{adj}\boldsymbol{P}}{\det \boldsymbol{P}}$, pak $\boldsymbol{P}\boldsymbol{D}\operatorname{adj}\boldsymbol{P}$ musí být dělitelné $\det \boldsymbol{P}$. Existují dvě skupiny prvků:

(*i*) na hlavní diagonále

$$\det \boldsymbol{P} \cdot \boldsymbol{a}_{11} = \sum_{i=1}^{n} \boldsymbol{\lambda}_i \mathbf{p}_{1i} \begin{vmatrix} \mathbf{p}_{11} & \cdots & \mathbf{p}_{1\,i-1} & \mathbf{p}_{1\,i+1} & \cdots & \mathbf{p}_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{p}_{n1} & \cdots & \mathbf{p}_{n\,i-1} & \mathbf{p}_{n\,i+1} & \cdots & \mathbf{p}_{nn} \end{vmatrix}$$

Je patrné, že se jedná o jednotlivé členy Laplaceova rozvoje $\boldsymbol{P}$ podle prvního řádku vynásobené postupně $\boldsymbol{\lambda}_1 \equiv \cdots \equiv \boldsymbol{\lambda}_n \mod \det \boldsymbol{P}$. Z toho důvodu podle lemmatu 1 jestliže $\boldsymbol{\lambda}_1 \equiv \cdots \equiv \boldsymbol{\lambda}_n \mod \det \boldsymbol{P}$, je a_{11} dělitelné $\det \boldsymbol{P}$ a tudíž i celé duální číslo. Obdobně pro ostatní prvky na diagonále.

(*ii*) prvky mimo hlavní diagonálu

Vezměme kupříkladu $\boldsymbol{a}_{12}$.

$$\det \boldsymbol{P} \cdot \boldsymbol{a}_{12} = \sum_{i=1}^{n} (-1)^i \boldsymbol{\lambda}_i \mathbf{p}_{1i} \begin{vmatrix} \mathbf{p}_{11} & \cdots & \mathbf{p}_{1\,i-1} & \mathbf{p}_{1\,i+1} & \cdots & \mathbf{p}_{1n} \\ \mathbf{p}_{31} & \cdots & \mathbf{p}_{3\,i-1} & \mathbf{p}_{3\,i+1} & \cdots & \mathbf{p}_{3n} \\ \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{p}_{n1} & \cdots & \mathbf{p}_{n\,i-1} & \mathbf{p}_{n\,i+1} & \cdots & \mathbf{p}_{nn} \end{vmatrix}$$

$$= \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (\boldsymbol{\lambda}_j - \boldsymbol{\lambda}_i) \cdot \mathbf{p}_{1i} \mathbf{p}_{1j}$$

$$\cdot \begin{vmatrix} \mathbf{p}_{31} & \cdots & \mathbf{p}_{3\,i-1} & \mathbf{p}_{3\,i+1} & \cdots & \mathbf{p}_{3\,j-1} & \mathbf{p}_{3\,j+1} & \cdots & \mathbf{p}_{3n} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \mathbf{p}_{n1} & \cdots & \mathbf{p}_{n\,i-1} & \mathbf{p}_{n\,i+1} & \cdots & \mathbf{p}_{n\,j-1} & \mathbf{p}_{n\,j+1} & \cdots & \mathbf{p}_{nn} \end{vmatrix},$$

takže jediná podmínka je dle lemmatu 1 opět kongruence $\boldsymbol{\lambda}_1 \equiv \boldsymbol{\lambda}_2 \equiv \cdots \equiv \boldsymbol{\lambda}_n \mod \det \boldsymbol{P}$.

Nyní dokažme, že matice $\boldsymbol{D}$ a $\boldsymbol{A}$ mají tytéž vlastní hodnoty. Dokazujeme tedy, že $\boldsymbol{A}$ má vlastní hodnoty $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_n$. Nechť $\boldsymbol{\lambda}$ je vlastní hodnotou $\boldsymbol{A}$. Potom $\boldsymbol{A}\vec{\boldsymbol{v}} = \boldsymbol{\lambda}\vec{\boldsymbol{v}}$ pro nějaký nenulový vektor $\vec{\boldsymbol{v}}$. Ale protože $\boldsymbol{A} = \boldsymbol{P}\boldsymbol{D}\boldsymbol{P}^{-1}$, potom

$$\boldsymbol{P}\boldsymbol{D}\boldsymbol{P}^{-1}\vec{\boldsymbol{v}} = \boldsymbol{\lambda}\vec{\boldsymbol{v}} \iff \boldsymbol{D}\boldsymbol{P}^{-1}\vec{\boldsymbol{v}} = \boldsymbol{P}^{-1}\boldsymbol{\lambda}\vec{\boldsymbol{v}} \iff \boldsymbol{D}\boldsymbol{P}^{-1}\vec{\boldsymbol{v}} = \boldsymbol{\lambda}\boldsymbol{P}^{-1}\vec{\boldsymbol{v}},$$

odkud vidíme, že $\boldsymbol{\lambda}$ je též vlastní hodnotou $\boldsymbol{D}$. Obdobně lze dokázat i obrácenou implikaci. Z toho důvodu mají matice $\boldsymbol{A}$ a $\boldsymbol{D}$ tytéž vlastní hodnoty. Vlastní hodnoty matice $\boldsymbol{D}$ jsou kořeny rovnice $\det(\boldsymbol{D} - \boldsymbol{\lambda}\boldsymbol{I}) = 0$, ale $\boldsymbol{D}$ sestává pouze z $\boldsymbol{\lambda}_i$ na hlavní diagonále, takže rovnice může být ekvivalentním způsobem přepsána jako

$$(\boldsymbol{\lambda}_1 - \boldsymbol{\lambda}) \cdot (\boldsymbol{\lambda}_2 - \boldsymbol{\lambda}) \cdot \cdots \cdot (\boldsymbol{\lambda}_n - \boldsymbol{\lambda}) = 0,$$

odkud vidíme, že vlastní hodnoty matice $\boldsymbol{D}$ (ale taky $\boldsymbol{A}$) jsou $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2, \ldots, \boldsymbol{\lambda}_n$, což jsme chtěli dokázat. □

Mřížová kryptografie

Mříže

Ještě předtím, než se pustíme do samotné konstrukce kryptosystému GGH, musíme nadefinovat několik pojmů a uvést věty s nimi související.

Definice 13. Nechť je nad $\mathbb{R}$ dáno n lineárně nezávislých vektorů $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$. Potom množinu

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} a_i \vec{v}_i; a \in \mathbb{Z} \right\}$$

nazveme *mříží* s basí $A = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$. Značíme $\mathcal{L}(A)$.

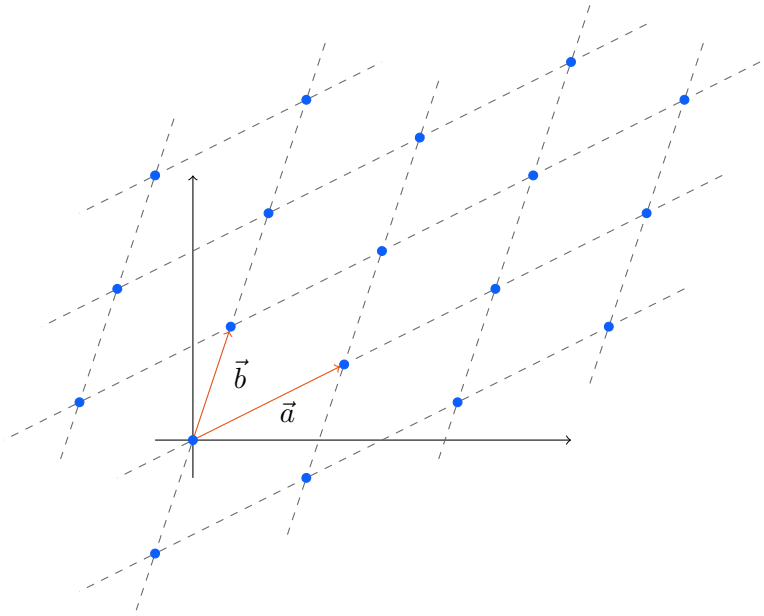
Poznámka. Někdy zápisem $\mathcal{L}(A)$, kde A je matice:

$$A = \begin{pmatrix} v_{11} & v_{21} & \ldots & v_{n1} \\ v_{12} & v_{22} & \ldots & v_{n2} \\ \vdots & \vdots & & \vdots \\ v_{1n} & v_{2n} & \ldots & v_{nn} \end{pmatrix}$$

rozumíme mříž generovanou vektory $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$.

Poznámka. Koncové body těchto vektorů vykreslují útvar připomínající mříž na dřevěném plotu či tradičním anglickém jablkovém koláči, odtud název (angl. *lattice*). [**lattice**]

Příklad 4. Jsou dány vektory $\vec{a} = (4, 2), \vec{b} = (1, 3)$. Na obrázku 1 jsou zaznačeny červeně, jednotlivé mřížové body (to jest body této mříže) jsou pak zaznačeny modře.



Obrázek 1: Mříž generována vektory $\vec{a}, \vec{b}$

Poznámka. My budeme používat hlavně mříže generované vektory ze $\mathbb{Z}^n$.

Kryptosystém je postaven na následující skutečnosti.

Věta 7. Nechť je dána matice A, jejíž vektory jsou sloupcově basí mříže $\mathcal{L}(A)$ a libovolná unimodulární matice M. Potom $\mathcal{L}(A) = \mathcal{L}(AM)$.

Důkaz. Označme $B = AM$. Protože M je maticí unimodulární, pak i M^{-1} je celočíselnou unimoduální maticí. Zjevně $A = BM^{-1}$ a $B = AM$, tedy $\mathcal{L}(A) \subseteq \mathcal{L}(B), \mathcal{L}(B) \subseteq \mathcal{L}(A)$, tedy $\mathcal{L}(A) = \mathcal{L}(B)$, takže $\mathcal{L}(A) = \mathcal{L}(AM)$, což jsme chtěli dokázat. □

Kryptosystém GGH

Zkratka „GGH“ pochází z příjmení jeho objevitelů: Goldreich, Goldwasser, Halevi.

Jedná se o kryptosystém s veřejným klíčem. Tento klíč je veřejně vystaven. Pokud chce někdo poslat zprávu, zašifruje ji pomocí předem domluvené ope-

race využívající tento veřejný klíč. Zpravidla se jedná o takovou operaci, jež se obtížně bez znalosti soukromého klíče invertuje. Takto zašifrovaná zpráva může být poslána. Recipient zprávu dešifruje podle předem domluvené operace využívající předem domluvený soukromý klíč. [**gghintr**]

Mějme n-dimensionální mříž $\mathcal{L}$ generovanou celočíselnými vektory $v_1, \ldots,$ v_n. Nic nám nebrání tyto vektory zapsat vedle sebe do matice následovně:

$$Z = \begin{pmatrix} v_{11} & v_{21} & \ldots & v_{n1} \\ v_{12} & v_{22} & \ldots & v_{n2} \\ \vdots & \vdots & & \vdots \\ v_{1n} & v_{2n} & \ldots & v_{nn} \end{pmatrix}$$

Tato matice Z bude spolu s libovolnou unimodulární maticí M téhož řádu soukromým klíčem. Z je zvolena „hezky“, to jest zpravidla s nízkými hodnotami.

Veřejným klíčem bude druhá, „ošklivá“ matice Y generující tutéž mříž $\mathcal{L}$, získaná jako $Y = ZM$. Alice chce poslat Bobovi milostné psaníčko vyjádřené vektorem $\vec{m} = (m_1, m_2, \ldots, m_n)$. K tomu si vymyslí dostatečně malý chybový vektor $\vec{e} = (e_1, e_2, \ldots, e_n)$. Jeho přesné vlastnosti jsou popsány ve větě 8. Zašifrovanou zprávu získáme jako $\vec{c} = Y\vec{m} + \vec{e}$.

Bob si zprávu dešifruje následovně:

$$\vec{d} = Z^{-1}\vec{c}$$
$$\vec{m} = M^{-1} \cdot \left\lfloor \vec{d} \right\rceil,$$

kde $\lfloor a \rceil$ značí klasické zaokrouhlení čísla a.

Příklad 5. Uveďme příklad tohoto šifrovacího algoritmu. Zvolme si

$$Z = \begin{pmatrix} 9 & 3 & 6 \\ 3 & 10 & 8 \\ 10 & 7 & 2 \end{pmatrix}, \; M = \begin{pmatrix} 642758 & 197757036 & 547515693 \\ -45807 & -14092427 & -39081807 \\ 729 & 224276 & 621928 \end{pmatrix},$$

přičemž $\det M = -1$. Potom spočteme matici Y:

$$Y = ZM = \begin{pmatrix} 5651775 & 1738881699 & 4814127384 \\ 1476036 & 454141046 & 1256704433 \\ 6108389 & 1879371923 & 5202828137 \end{pmatrix}$$

Zašifrujme nyní zprávu „GGH“, $\vec{m} = (71, 71, 72)$ s chybovým vektorem $\vec{e} = (1, 1, 1)$.

$$\vec{c} = Y\vec{m} + \vec{e} = \begin{pmatrix} 470479048303 \\ 122831531999 \\ 508472728017 \end{pmatrix}$$

Tato zpráva je nyní poslána příjemci. Ten ji dešifruje následovně.

$$\vec{d} = Z^{-1}\vec{c} = \begin{pmatrix} 53507515270{,}0625 \\ -3817704717{,}9618\overline{05} \\ 60754171{,}0538\overline{194} \end{pmatrix}$$

$$\vec{m} = M^{-1}\left\lfloor \vec{d} \right\rceil = M^{-1}\begin{pmatrix} 53507515270 \\ -3817704718 \\ 60754171 \end{pmatrix} = \begin{pmatrix} 71 \\ 71 \\ 72 \end{pmatrix}.$$

Odvození. Ukažme, proč kryptosystém funguje. Dešifrovaná zpráva $\vec{m}$ se dá bez chybového vektoru vyjádřit jako

$$\vec{m} = M^{-1}Z^{-1}\vec{c} = M^{-1}Z^{-1}Y\vec{m} = M^{-1}Z^{-1}ZM\vec{m} = \vec{m}.$$

Takový kryptosystém by však nefungoval, protože zpráva $Y\vec{m}$ se dá dešifrovat jako $Y^{-1}Y\vec{m}$. $Y\vec{m}$ je totiž bodem mříže $\mathcal{L}(Y)$. Přičtením chybového vektoru se tedy „posuneme mimo ni“. Chybový vektor musí být dostatečně malý, abychom se při zaokrouhlování nedostali k jinému bodu této mříže.

Věta 8. Pro danou generátorovou matici Z lze omezit chybový vektor následovně. Nechť l je největší součet absolutních hodnot prvků řádku matice Z^{-1}. Pak $\sigma = \frac{1}{2l}$ a $\vec{e}_i \in (-\sigma, \sigma), i \in \{1, \ldots, n\}$.

Důkaz. Vyjádřeme dešifrovanou zprávu $\vec{m}$.

$$\begin{aligned}\vec{m} &= M^{-1} \cdot \left\lfloor Z^{-1}\vec{c} \right\rceil = M^{-1} \cdot \left\lfloor Z^{-1} \cdot (Y\vec{m} + \vec{e}) \right\rceil \\ &= M^{-1} \cdot \left\lfloor Z^{-1} \cdot (ZM\vec{m} + \vec{e}) \right\rceil = M^{-1} \cdot \left\lfloor M\vec{m} + Z^{-1}\vec{e} \right\rceil,\end{aligned}$$

takže musí $\left\lfloor Z^{-1}\vec{e} \right\rceil = \vec{o}$, protože $M\vec{m}$ je vždy celočíselný vektor. Předpokládejme, že chybový vektor je největšího možného tvaru $\vec{e} = (\sigma, \ldots, \sigma)$. Bez újmy na obecnosti považujme za největší první řádek matice Z^{-1}, již si označíme následovně:

$$\left\lfloor \begin{pmatrix} a & b & c & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ \cdot & \cdot & \cdot & \cdots \\ & \vdots & & \end{pmatrix} \begin{pmatrix} \sigma \\ \sigma \\ \sigma \\ \vdots \end{pmatrix} \right\rceil = \vec{o},$$

v absolutní hodnotě největší souřadnice vektoru $\vec{e}$ tedy bude ta první, dostáváme následující rovnici

$$\begin{aligned}|a\sigma + b\sigma + c\sigma + \cdots| &< \frac{1}{2} \\ |\sigma(a + b + c + \cdots)| &< \frac{1}{2}\end{aligned}$$

a pokud $|\sigma| < \frac{1}{2(a+b+c+\cdots)}$, potom

$$\left| \frac{a + b + c + \cdots}{2(a + b + c + \cdots)} \right| < \frac{1}{2},$$

čímž jsme tvrzení dokázali. □

Tímto způsobem sice přijdeme o některé možné hodnoty chybového vektoru, vzorec je zato jednodušší.

Aplikace duálních čísel

Ukážeme, že kryptosystém bude fungovat i při konstrukci nad $\mathbb{Z}[\varepsilon]$. Uveďme tedy příslušné definice, které k zavedení budeme potřebovat.

Věta 9. Matice $\boldsymbol{M}$ nad $\mathbb{Z}[\varepsilon]$ je unimodulární právě tehdy, když $\det \boldsymbol{M} = \pm 1 + k\varepsilon, k \in \mathbb{Z}$.

Důkaz. Nejprve ukažme, že $\det \operatorname{adj} \boldsymbol{M} = \det(\boldsymbol{M})^{n-1}$, kde n je řád matice $\boldsymbol{M}$. Pro adjugovanou matici platí

$$\begin{aligned} \boldsymbol{M} \cdot \operatorname{adj} \boldsymbol{M} &= \det(\boldsymbol{M}) \cdot \boldsymbol{I} \\ \det(\boldsymbol{M}) \cdot \det(\operatorname{adj}(\boldsymbol{M})) &= \det(\boldsymbol{M})^n \\ \det(\operatorname{adj}(\boldsymbol{M})) &= \det(\boldsymbol{M})^{n-1}, \end{aligned}$$

takže potom

$$\begin{aligned} \boldsymbol{M}^{-1} &= \frac{1}{\det \boldsymbol{M}} \cdot \operatorname{adj} \boldsymbol{M} \\ \det \boldsymbol{M}^{-1} &= \frac{1}{\det \boldsymbol{M}} \cdot \det \operatorname{adj} \boldsymbol{M} = \frac{\det(\boldsymbol{M})^{n-1}}{\det \boldsymbol{M}} = \det(\boldsymbol{M})^{n-2}, \end{aligned}$$

jenže při vydělení duálním číslem $(1+a\varepsilon)^2$ je $\det \boldsymbol{M}^{-1}$ stále tvaru $1+l\varepsilon, l \in \mathbb{Z}$, protože dělit duálním číslem $1 + a\varepsilon$ je totéž jako násobit číslem $1 - a\varepsilon$, takže po vynásobení vyjde celé číslo. □

Důsledek 3. Nechť je dána unimodulární matice $\boldsymbol{M}$ s $\det \boldsymbol{M} = \pm 1 + k\varepsilon, k \in \mathbb{Z}$. Pak $\det \boldsymbol{M}^{-1} = \pm 1 - k\varepsilon$.

Důkaz. Pro unimodulární matici platí $\boldsymbol{M}\boldsymbol{M}^{-1} = \boldsymbol{I}$, pro jejich determinanty pak $\det \boldsymbol{M} \cdot \det \boldsymbol{M}^{-1} = 1$, řešíme tedy rovnici $(1 + k\varepsilon)(1 + l\varepsilon) = 1 + 0\varepsilon$, kde k je parametr a l je neznámá. Odtud dostáváme soustavu rovnic

$$\begin{aligned} 1 &= 1, \\ l + k &= 0, \end{aligned}$$

takže opravdu $l = -k$. □

Definice 14. Nechť je nad $\mathbb{R}[\varepsilon]$ dáno n lineárně nezávislých vektorů $\vec{\boldsymbol{v}}_1, \vec{\boldsymbol{v}}_2, \ldots, \vec{\boldsymbol{v}}_n$. Potom množinu

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} \boldsymbol{a}_i \vec{\boldsymbol{v}}_i ; \boldsymbol{a} \in \mathbb{Z}[\varepsilon] \right\}$$

nazveme *duální mříží* s basí $\boldsymbol{A} = \{\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n\}$. Značíme $\mathcal{L}(\boldsymbol{A})$.

Všimněme si, že duální jsou jak vektory, tak koeficienty jednotlivých lineárních kombinací. Duální mříž je tedy na rozdíl od celočíselné mříže jen R-modulem (protože $\mathbb{Z}[\varepsilon]$ není těleso, ale jen okruh), nikoliv vektorovým prostorem.

Věta 10. Nechť je dána matice $\boldsymbol{A}$ s prvky ze $\mathbb{Z}[\varepsilon]$, jejíž vektory jsou sloupcově basí mříže $\mathcal{L}(\boldsymbol{A})$ a libovolná duální unimodulární matice $\boldsymbol{M}$. Potom $\mathcal{L}(\boldsymbol{A}) = \mathcal{L}(\boldsymbol{AM})$.

Důkaz. Důkaz je proveden tímtéž způsobem jako u věty 7. □

Definice 15. Nechť $\boldsymbol{a} \in \mathbb{Z}[\varepsilon]$. Pak $\lfloor \boldsymbol{a} \rceil = \lfloor a_0 \rceil + \lfloor a_1 \rceil \, \varepsilon$.

Potom kryptosystém GGH funguje stejným způsobem. Uveďme tedy příklad.

Příklad 6. Zvolme si

$$\boldsymbol{Z} = \begin{pmatrix} 150 + 7\varepsilon & 8 + 5\varepsilon & 6 + 10\varepsilon \\ 4 + 5\varepsilon & 405 + 9\varepsilon & 8 + 8\varepsilon \\ 10 + 6\varepsilon & 7 + 7\varepsilon & 390 + 5\varepsilon \end{pmatrix},$$

$$\boldsymbol{M} = \begin{pmatrix} -94 + 667\varepsilon & 692 - 234\varepsilon & -753 - 893\varepsilon \\ -21 + 468\varepsilon & 155 + 368\varepsilon & -168 - 126\varepsilon \\ -8 - 906\varepsilon & 59 - 684\varepsilon & -64 + 688\varepsilon \end{pmatrix},$$

kde $\det \boldsymbol{M} = -1 - 531847\varepsilon$. Nilpotentní část je zvolena zcela náhodně. Pak

$\boldsymbol{Y}$ je spočteno jako

$$\boldsymbol{Y} = \boldsymbol{ZM} = \begin{pmatrix} -18862 + 88468\varepsilon & 274237 - 95198\varepsilon & -288698 - 345309\varepsilon \\ -4210 + 70032\varepsilon & 61431 + 152016\varepsilon & -64406 - 43198\varepsilon \\ -1604 - 131901\varepsilon & 23383 - 279409\varepsilon & -24536 + 257484\varepsilon \end{pmatrix}$$

Zašifrujme zprávu „Morava“, representovanou jako vektor $\vec{\boldsymbol{m}} = (77 + 111\varepsilon, 114 + 97\varepsilon, 118 + 97\varepsilon)$. Všimněme si, že v tomtéž řádu ($n = 3$) můžeme použít dvakrát více znaků, než kdybychom pracovali v $\mathbb{Z}$. Chybový vektor nechť je $\vec{\boldsymbol{e}} = (1 + \varepsilon, 1 + \varepsilon, 1 + \varepsilon)$.

$$\vec{\boldsymbol{c}} = \boldsymbol{Y}\vec{\boldsymbol{m}} + \vec{\boldsymbol{e}} = \begin{pmatrix} -2121585 - 3426273\varepsilon \\ 30878578 + 15696582\varepsilon \\ -32467277 - 41803104\varepsilon \end{pmatrix}$$

Po dešifrování zjistíme, že zpráva je totožná s tou, již jsme poslali.

Poznámka. Obdobně je tento kryptosystém definován nad Gaussovými celými čísly.

Nyní lze omezit chybový vektor podobně jako v $\mathbb{Z}$.

Věta 11. Pro danou generátorovou matici $\boldsymbol{Z}$ lze omezit chybový vektor následovně. Nechť l_0 je největší součet absolutních hodnot regulárních částí prvků řádku matice $\boldsymbol{Z}^{-1}$ a l_1 je největší součet absolutních hodnot nilpotentních částí prvků řádků téže matice. Pak $\sigma_0 = \frac{1}{2l_0}$ a $\sigma_1 = \frac{|l_0 - l_1|}{2l_0^2}$, přičemž $\vec{\boldsymbol{e}}_{i0} \in (-\sigma_0, \sigma_0)$ a $\vec{\boldsymbol{e}}_{i1} \in (-\sigma_1, \sigma_1), i \in \{1, \ldots, n\}$ pokud $\sigma_1 \neq 0$, v opačném případě $\vec{\boldsymbol{e}}_{i1} = 0$.

Důkaz. Obdobně jako u věty 8 dostáváme $\lfloor \boldsymbol{Z}^{-1}\vec{\boldsymbol{e}} \rceil = \vec{\boldsymbol{o}}$, předpokládejme tedy, že chybový vektor je největšího možného tvaru $\vec{\boldsymbol{e}} = (\sigma_0 + \sigma_1, \ldots, \sigma_0 + \sigma_1)$ a l jsou součty prvků prvního řádku. Pak největší souřadnice vektoru $\vec{\boldsymbol{e}}$ je

$$|\boldsymbol{\sigma}(\boldsymbol{a} + \boldsymbol{b} + \boldsymbol{c} + \cdots)| < \frac{1}{2} + \frac{1}{2}\varepsilon,$$

dostáváme tedy soustavu rovnic

$$|\sigma_0 l_0| < \frac{1}{2}$$
$$|\sigma_0 l_1 + \sigma_1 l_0| < \frac{1}{2},$$

po dosazení za $\boldsymbol{\sigma}$:

$$|\sigma_0 l_0| < \left|\frac{l_0}{2l_0}\right| = \frac{1}{2},$$
$$|\sigma_0 l_1 + \sigma_1 l_0| < \left|\frac{l_1}{2l_0} + \frac{l_0(l_0 - l_1)}{2l_0^2}\right| = \left|\frac{l_1 + l_0 - l_1}{2l_0}\right| = \frac{1}{2},$$

čímž jsme tvrzení dokázali. □

Implementace v C++

Pro názornou ukázku tohoto kryptosystému na složitějších maticích jsem vytvořil skript jako nadstavbu knihovny Eigen a cppduals.

Jako globální proměnnou zvolíme řád matice, se kterou budeme pracovat. V této implementaci je k disposici několik tříd: `Vector`, `Matrix`, `Translator` a `Cryptosystem`.

Pro demonstraci uveďme jednoduchý kód, jenž zašifruje a dešifruje danou zprávu:

```
#include <iostream>
#include <Eigen/Dense>
#include <duals/dual>
#include <vector>
#include <time.h>
#include "Cryptosystem.h"
#include "Translator.h"
#include <iomanip>
```

```
using namespace duals;
using namespace Eigen;
using namespace std;

const short N = 3;

int main() {
// inicialisace srand
srand(time(0));

// vytvoreni matice Z radu N
Mat<dual<long long int>> Z(N,N);

// vytvoreni vektoru m, e, ciphered, decrypted
Vect<dual<long long int>> m(N), e(N), ciphered(N),
decrypted(N);

// navoleni matice Z
Z <<
  150+7_e,  8+5_e,     6+10_e,
  4+5_e,    405+9_e,   8+8_e,
  10+6_e,   7+7_e,     390+5_e;

// matici M lze do funkce poslat bud explicitne zadanou,
// nebo ji nechat generovat;
// a to bud jen regularni, nebo i nilpotentni cast
unimodularMatrixData unimodData;

// matice M

// regularni cast je unimodularni
```

```
unimodData.unimodrpart = true;
// nilpotentni cast je (pseudo)nahodna
unimodData.unimoddpart = false;
// nelze posilat prazdnou matici
unimodData.matrix.push_back(0+0_e);

// zadani zpravy
m << 77+111_e, 114+97_e, 118+97_e;

// zvoleni chyboveho vektoru
e << 74+0_e, 74+0_e, 74+0_e;

// stvoreni instance kryptosystemu
CryptoSystem<dual<long long int>> system(N, Z, unimodData);

// zasifrovani zpravy
ciphered = system.cipher(m, e);

// vytisknuti zasifrovane zpravy
cout << "ciphered" << endl << ciphered << endl << endl;

// desifrovani zpravy
decrypted = system.decrypt(ciphered);

// vytisknuti desifrovane zpravy
cout << "decrypted" << endl << decrypted << endl;
}
```

Výstup pak vypadá následovně:

```
ciphered
(-186512+5958227_e)  (-1020404-8276735_e) (18198120+28904310_e)
```

```
decrypted
(77+111_e) (114+97_e) (118+97_e)
```

Pomocí tohoto skriptu lze jednoduše šifrovat a dešifrovat dané zprávy. Bylo by možné jej použít v praxi, např. pro zašifrované psaní zpráv. Taktéž jsem implementoval překlad zprávy ze souboru a její následné zašifrování.

Nguyenův útok

Pouhé dva roky po prvním zveřejnění kryptosystému GGH došlo k jeho napadení, známému jako Nguyenův útok. Objasněme, v čem útok spočívá a ukažme, jestli jej aplikace duálních čísel nějak eliminuje.

V původním návrhu tohoto kryptosystému se používal chybový vektor tvaru $\vec{e} = (\sigma, \ldots, \sigma)$ nebo s hodnotami opačnými. Za těchto předpokladů lze zjistit informace o zprávě.

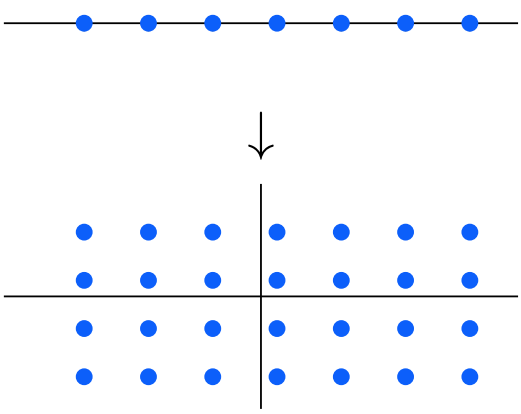
Označme $\vec{\sigma} = (\sigma, \ldots, \sigma)$. Pak $\vec{c} + \vec{\sigma} = Y\vec{m} + \vec{e} + \vec{\sigma}$, kde každá ze souřadnic $\vec{e} + \vec{\sigma}$ je buď 0 nebo 2σ. Modulo 2σ pak rovnice vypadá následovně:

$$\vec{c} + \vec{\sigma} \equiv Y\vec{m} \mod 2\sigma,$$

takže při vynásobení maticí Y^{-1} zleva (Y známe z veřejného klíče) lze zjistit infromace o původní zprávě. Poté přičítáme k jednotlivým souřadnicím násobky 2σ, dokud nevyjde smysluplná zpráva. Tento postup nebude fungovat, pokud $\det Y \equiv 0 \mod 2\sigma$.

Pokud se jako chybový vektor nepoužívá $(\sigma, \ldots, \sigma)$, přičítáme postupně $\sigma, \sigma - 1, \sigma - 2, \ldots$, dokud se nedostaneme ke smysluplné zprávě. [**ggh**]

V duálních číslech je ale situace horší. Počet možností totiž oproti konstrukci nad celými čísly kvůli přítomnosti nilpotentní části stoupá exponenciálně, jak je vidět na obrázku 2. Navíc operace *modulo* nemusí být v $\mathbb{Z}[\varepsilon]$ vždy definována. Tím je Nguyenův útok alespoň velice znehodnocen, pokud není nemožný vůbec.



Obrázek 2: Počty chybových vektorů v $\mathbb{Z}$ a $\mathbb{Z}[\varepsilon]$

Representace zprávy jako sekvence čísel

Při posílání zprávy je potřeba ji přeložit ze sekvence písmen do sekvence čísel. Jedině tak ji totiž můžeme zašifrovat.

V běžné praxi se pro to používá tabulka ASCII (z angl. *American Standard Code for Information Interchange*). Pro duální čísla můžeme algoritmus upravit následovně: každé písmeno zprávy je podle tabulky převedeno na číslo a tvoří pak postupně regulární a nilpotentní část jednotlivých souřadnic vektoru $\vec{\boldsymbol{m}}$. Názorné vysvětlení nabízí následující příklad.

Příklad 7. Předveďme proces zašifrování zprávy „`Brno <3`“ do matice řádu 2. Výsek z tabulky ASCII je níže.

znak	...	@	A	B	C	...	a	b	c	d	e	...
ASCII kód	...	64	65	66	67	...	97	98	99	100	101	...

Obrázek 3: Výsek z tabulky ASCII

Uvedeným postupem lze jednoznačně převést každou zprávu na šifrovatelný vektor a naopak.

$$\begin{array}{cccc} \mathrm{B} & 66 & & \\ \mathrm{r} & 114 & & \\ \mathrm{n} & 110 & & \\ \mathrm{o} & \to\ 111 & \to & \begin{pmatrix} 66+114\varepsilon \\ 110+111\varepsilon \\ 32+60\varepsilon \\ 51+0\varepsilon \end{pmatrix} \\ & 32 & & \\ < & 60 & & \\ 3 & 51 & & \end{array}$$

Obrázek 4: Překlad zprávy do vektoru $\vec{\boldsymbol{m}}$

Závěr

V první části této práce jsme se zaměřili na představení pojmu duálních čísel a jejich základních vlastností jako je dělitelnost, kongruence či odmocnina. Po uvedení základních pojmů lineární algebry jsme zobecnili Towse-Campbellův algoritmus pro generování celočíselných matic s celočíselnými vlastními hodnotami.

Ve druhé části jsme pak prozkoumali duální unimodulární matice a jejich vliv na generátorové matice mříže. Zjistili jsme, že jich lze využít pro konstrukci vylepšeného kryptosystému GGH, který je bezpečnější než ten původní, konstruovaný nad celými čísly.

Na základě toho jsme vytvořili program v C++ aplikující námi předkládanou a v této práci dokázanou teorii do praxe. Tento program lze použít pro posílání šifrovaných zpráv a jejich opětovné dešifrování. Navíc jím lze převádět a následně šifrovat zprávy z textového souboru.

Demonstrovali jsme rozdíl v Nguyenově útoku v celých a duálních číslech. Tento typ útoku se v duálních číslech ovšem jeví jako nepoužitelný. Z toho důvodu je kryptosystém představený v této práci mnohem bezpečnější než ten stávající nad celými čísly.

Seznam obrázků